

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
MARSHALL DIVISION**

TAASERA LICENSING LLC,	§	Case No.
	§	
Plaintiff,	§	
	§	<b><u>JURY TRIAL DEMANDED</u></b>
v.	§	
	§	
CHECK POINT SOFTWARE	§	
TECHNOLOGIES LTD.,	§	
	§	
Defendant.	§	

**COMPLAINT FOR PATENT INFRINGEMENT**

Plaintiff Taasera Licensing LLC (“Taasera Licensing” or “Plaintiff”) for its Complaint against Defendant Check Point Software Technologies Ltd. (“Check Point” or “Defendant”) alleges as follows:

**THE PARTIES**

1. Taasera Licensing is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business located at 100 West Houston Street, Marshall, Texas 75670.

2. Upon information and belief, Defendant Check Point Software Technologies Ltd. is corporation organized under the laws of the Country of Israel, with its principal place of business at Shlomo Kaplan Street 5, Tel Aviv-Yafo, 6789159, Israel. Upon information and belief, Defendant may be served pursuant to the provisions of the Hague Convention. Upon information and belief, Check Point does business in Texas and in the Eastern District of Texas, directly or through intermediaries.

### **JURISDICTION**

3. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq.* This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over Defendant. Defendant regularly conducts business and has committed acts of patent infringement and/or has induced acts of patent infringement by others in this Judicial District and/or has contributed to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States.

5. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391 because, among other things, Defendant is a defendant not resident in the United States, and thus may be sued in any judicial district pursuant to 28 U.S.C. § 1391(c)(3).

6. Defendant is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and Judicial District, including (a) at least part of its past infringing activities, (b) regularly doing or soliciting business in Texas, and/or (c) engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in Texas.

### **PATENTS-IN-SUIT**

7. On January 11, 2005, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 6,842,796 (the "'796 Patent") entitled "Information Extraction from Documents with Regular Expression Matching." A true and correct copy of the '796 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=6842796>.

8. On December 4, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,327,441 (the "'441 Patent") entitled "System and Method for

Application Attestation.” A true and correct copy of the ’441 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=8327441>.

9. On February 10, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,955,038 (the “’038 Patent”) entitled “Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities.” A true and correct copy of the ’038 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=8955038>.

10. On March 24, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,990,948 (the “’948 Patent”) entitled “Systems and Methods for Orchestrating Runtime Operational Integrity.” A true and correct copy of the ’948 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=8990948>.

11. On July 28, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,092,616 (the “’616 Patent”) entitled “Systems and Methods for Threat Identification and Remediation.” A true and correct copy of the ’616 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=9092616>.

12. On March 28, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,608,997 (the “’997 Patent”) entitled “Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities.” A true and correct copy of the ’997 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=9608997>.

13. On March 20, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,923,918 (the “’918 Patent”) entitled “Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities.” A true

and correct copy of the '918 Patent is available at <http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=9923918>.

14. Taasera Licensing is the sole and exclusive owner of all right, title, and interest in the '796 Patent, the '441 Patent, the '038 Patent, the '948 Patent, the '616 Patent, the '997 Patent, and the '918 Patent (collectively, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Taasera Licensing also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

### **FACTUAL ALLEGATIONS**

15. The Patents-in-Suit generally cover systems and methods for network security systems.

16. Four of the Patents-in-Suit were invented by International Business Machines ("IBM"). IBM pioneered the field of network security. Every year, IBM spends billions of dollars on research and development to invent, market, and sell new technology, and IBM obtains patents on many of the novel inventions that come out of that work, including the Patents-in-Suit. The four patents invented by IBM are the result of the work from 4 different researchers, spanning over a decade.

17. Three of the Patents-in-Suit were developed by TaaSera, Inc. TaaSera, Inc. was a leader in preemptive breach detection systems, and comprised of security architects and subject matter experts with decades of experience in firewalls, intrusion detection, security event management, malware analysis, and endpoint security. The TaaSera, Inc. patents identify patterns of malicious coordinated network and endpoint behaviors.

18. The '796 Patent generally relates to technology that extracts information from documents with regular expression matching. The technology described in the '796 Patent was developed by Geoffrey G. Zweig and Mukund Padmanabhan of IBM.

19. The '441 Patent generally relates to technology for application attestation. The technology described in the '441 Patent was developed by Srinivas Kumar and Gurudatt Shashikumar of TaaSera, Inc.

20. The '038 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the '038 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

21. The '948 Patent generally relates to technology that provides runtime operational integrity profiles identifying a threat level of subjects or applications. The technology described in the '948 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc.

22. The '616 Patent generally relates to technology that provides integrity profiles identifying a threat level of a system. The technology described in the '616 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc.

23. The '997 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the '997 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

24. The '918 Patent generally relates to technology that controls access to computing resources based on known security vulnerabilities. The technology described in the '918 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

25. Defendant has infringed and continues to infringe one or more of the Patents-in-Suit by making, using, selling, offering to sell, and/or importing, and by actively inducing others

to make, use, sell, offer to sell, and/or import products that implement the network security inventions claimed in the Patents-in Suit. For example, the Accused Products include at least Check Point Next Generation Firewalls, Check Point Data Loss Prevention Software Blade, and Checkpoint Infinity Portal with Harmony Endpoint.

26. TaaSera, Inc. manufactured commercial and academic versions of its NetTrust Security Appliance. NetTrust combined breach detection with security analytics to identify hidden threatening network behaviors. The analytics engine analyzed behavioral profiles, threat patterns, and contextual evidence to rank systems by their risk of breach.

27. Upon information and belief, Taasera Licensing and its predecessors have complied with the requirements of 35 U.S.C. § 287(a).

**COUNT I**  
**(Infringement of the '796 Patent)**


28. Paragraphs 1 through 27 are incorporated by reference as if fully set forth herein.

29. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '796 Patent.

30. Defendant has and continues to directly infringe the '796 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '796 Patent. Such products incorporate the Data Loss Prevention (DLP) feature and include at least the Check Point Next Generation Firewalls and the Check Point Data Loss Prevention Software Blade (the "'796 Accused Products") which practice a method of automatically processing an input sequence of data symbols, the method comprising the steps of: identifying at least one regularly identifiable expression in the input sequence of data symbols, wherein the at least one regularly identifiable expression represents a

pattern that is matchable in accordance with a programming language that supports such a regularly identifiable expression; identifying at least a portion of information associated with the at least one regularly identifiable expression; and extracting the portion of information.

31. Every '796 Accused Product practices automatically processing an input sequence of data symbols. For example, the Check Point Data Loss Prevention Software Blade incorporates DLP rules.


Data Loss Prevention Software Blade | Datasheet

## CHECK POINT DATA LOSS PREVENTION SOFTWARE BLADE

### CHECK POINT DLP SOFTWARE BLADE

Check Point Data Loss Prevention (DLP) Software Blade™ combines technology and processes to revolutionize DLP, helping businesses to pre-emptively protect sensitive information from unintentional loss, educating users on proper data handling policies and empowering them to remediate incidents in real-time.

### KEY BENEFITS

- **Prevents data loss of critical business information:**  
UserCheck™ technology empowers users to remediate incidents in real time.
- **Combines technology and processes to make DLP work:**  
Innovative MultiSpect™ data classification engine combines users, content and process that deliver unrivaled accuracy.
- **Easy deployment for immediate data loss prevention:**  
Protect sensitive data from day-1 with pre-configured policies and the broadest support for file formats and data types.

### INSIGHTS

In today's world of increasing data loss events, organizations have little choice but to take action to protect sensitive data. Confidential employee and customer data, legal documents, and intellectual property are being exposed. Organizations are challenged with effectively addressing this without impeding employee productivity or overloading IT staff. Technology is evolving, but ultimately ineffective in understanding user intentions. Even more difficult is trying to protect sensitive data without the long deployments, painful administration and high costs often associated with traditional DLP products.

### OVERVIEW

Check Point revolutionizes DLP by combining technology and processes to move businesses from passive detection to active Data Loss Prevention. Innovative MultiSpect™ data classification combines user, content and process information to make accurate decisions, while UserCheck™ technology empowers users to remediate incidents in real time. Check Point's self-educating network-based DLP solution frees IT/security personnel from incident handling and educates users on proper data handling policies—protecting sensitive corporate information from both intentional and unintentional loss.

### CHECK POINT USERCHECK™

Check Point UserCheck empowers users to remediate incidents in real time. This innovative technology alerts users of suspected breaches, allowing for instant remediation, and allows quick authorization of legitimate communications.

UserCheck™ empowers users to self-administer incident handling, with options to send, discard or review the issue, improving security by raising awareness of data use policies. Real-time notification based either on a pop-up from a thin agent or via a dedicated email sent to end user (no need to install agent). Organizations benefit in several ways:


- ✓ **Full prevention**—enables a practical move from detection to prevention
- ✓ **Self-educating system**—doesn't require IT / security personnel in incident handling while educating the users on proper data sharing policies

<sup>1</sup> <https://www.checkfirewalls.com/datasheets/data-loss-prevention-dlp-datasheet.pdf>

32. Every '796 Accused Product practices identifying at least one regularly identifiable expression in the input sequence of data symbols, wherein the at least one regularly identifiable expression represents a pattern that is matchable in accordance with a programming language that supports such a regularly identifiable expression. For example, Check Point Data Loss Prevention Software Blade enforces DLP rules created using patterns/regular expressions.

### Protecting Data by Pattern

You can create a regular expression that will be matched against content in data transmissions. Transmissions that contain strings that match the pattern in their data are matched.



**Note** - Use the Check Point supported regular expression syntax.

**To create a data type representation of a pattern:**

1. In the **Data Type Wizard**, select **Pattern (regular expressions)**.
2. Click **Next**.
3. Enter a pattern to match against content.
4. Click **Add**.
5. Enter as many regular expressions as you want in this data type.
6. Decide whether data should match the data type if the pattern is matched even once, or if it should be allowed until a given number of times.  
For example, if you want to ensure that no one can send an email that contains a complete price-list of five products, you would set the pattern to `^[0-9]+\.[0-9]{2}?$` and you would set the **Number of occurrences** to **5**.
7. Click **Next**.
8. Click **Finish**; or if you want to add more parameters to the data type, select the checkbox and then click **Finish**.

2

33. Every '796 Accused Product practices identifying at least a portion of information associated with the at least one regularly identifiable expression. For example, Check Point Data Loss Prevention Software Blade extracts information to use in the notification of a match to an DLP rule.

<sup>2</sup> [https://dl3.checkpoint.com/paid/14/142e811ba1bcd2be49631cb1df253916/CP\\_R80.10\\_DataLossPrevention\\_AdminGuide.pdf?HashKey=1635522712\\_391ef7445f78ded080308233edd69fec&xtn=.pdf](https://dl3.checkpoint.com/paid/14/142e811ba1bcd2be49631cb1df253916/CP_R80.10_DataLossPrevention_AdminGuide.pdf?HashKey=1635522712_391ef7445f78ded080308233edd69fec&xtn=.pdf)

<b>Enforcement</b>	
<b>Types</b>	<ul style="list-style-type: none"> <li>✓ Ask User (self prevent with UserCheck) – places message in quarantine, send notification to end user, request self-remediation.</li> <li>✓ Prevent – block message from being sent and notify the end-user.</li> <li>✓ Detect – log events.</li> </ul>
<b>UserCheck™</b>	<ul style="list-style-type: none"> <li>✓ Enabled and customized per policy with individual editable notification to end-user (multi-language)</li> <li>✓ Self learning – prevents recurring incident management within same mail threat</li> <li>✓ Two notification methods – email reply (no need for agent installation), or system tray pop-up (requires thin agent installation)</li> </ul>
<b>Enforcement Features</b>	<ul style="list-style-type: none"> <li>✓ Policy exceptions per user, user group, network, protocol, or data type</li> <li>✓ Send notification of potential breaches to owner of data asset (e.g. CFO for financial documents)</li> <li>✓ Log all incidents – with option to correlate events and audit incidents</li> </ul>
<b>View Incident</b>	<ul style="list-style-type: none"> <li>✓ Granular administrator permissions provide control over who can see DLP data</li> <li>✓ Sensitive data in DLP event logs can be masked (e.g. only the last four digits of credit card numbers are shown)</li> </ul>
<b>Log All Emails</b>	<ul style="list-style-type: none"> <li>✓ An audit log is created each time a captured message is viewed</li> <li>✓ All outgoing emails (including non-incidents) are logged for sender, recipients and subject</li> </ul>

3

34. Defendant has and continues to indirectly infringe one or more claims of the '796 Patent by knowingly and intentionally inducing others, including Check Point subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the '796 Accused Products (*e.g.*, products incorporating the DLP feature).

35. Defendant, with the knowledge that these products, or the use thereof, infringe the '796 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '796 Patent by providing these products to end-users for use in an infringing manner.

36. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '796 Patent, but while remaining willfully blind to the infringement.

<sup>3</sup> <https://www.checkfirewalls.com/datasheets/data-loss-prevention-dlp-datasheet.pdf>

37. Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '796 Patent in an amount to be proved at trial.

38. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '796 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

**COUNT II**  
**(Infringement of the '441 Patent)**


39. Paragraphs 1 through 27 are incorporated by reference as if fully set forth herein.

40. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '441 Patent.

41. Defendant has and continues to directly infringe the '441 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '441 Patent. Such products incorporate the Behavioral Guard with Forensic Reports feature and include at least the Check Point Infinity Portal with Harmony Endpoint (the "'441 Accused Products") which practice a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server, comprising: receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components; generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution

context and the received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application.

42. Every '441 Accused Product practices a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server. For example, Check Point Infinity incorporates real-time threat prevention engines to prevent cyber threats.



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

Check Point Infinity | Data Sheet

WELCOME TO THE FUTURE OF CYBER SECURITY

## CHECK POINT INFINITY

A consolidated cyber security architecture



### INFINITY AT-A-GLANCE

#### Benefits

- Improves security with a consolidated, unified architecture
- Offers real-time threat prevention against known and zero-day threats
- Leverages shared threat intelligence and automation across all enforcement points
- Provides full visibility into organization's threat posture with single, unified management console
- Reduces TCO by 20% and increases operational efficiency by 50%

#### Features

**Consolidated**  
Unified protection across the entire IT infrastructure: networks, cloud, endpoints, mobile and IoT devices.

**Threat Prevention**  
Uses 64 different threat prevention engines to block against known and zero-day threats, powered by shared threat intelligence.

**Efficiency**  
Unified security management, completely automated and seamlessly integrated.

### Changing Business Needs. Rising Threats.

Business needs have changed as most organizations are moving to the Cloud, initiating digital transformation projects, enabling significantly more remote workers, and adding new devices to the network every day. Meanwhile, enterprise security teams are chronically understaffed, working with limited budgets, and using aging tools. Protecting your organization from new, sophisticated cyber attacks has never been more challenging.

Check Point Infinity is the first modern, consolidated, cyber security architecture built to prevent sophisticated Fifth Generation attacks across networks, cloud deployments, endpoints, mobile and IoT devices. Infinity enables organizations to solve security gaps, reduce risk, and lower total cost of ownership.

### Protection for the Entire IT Infrastructure

Infinity enables organizations to prevent cyber threats, simplify security management, and boost efficiency. Infinity's single management console centrally correlates a wide range of events across all network environments, cloud services and mobile infrastructures, with Check Point's pre-emptive threat prevention technologies blocking the most sophisticated attacks before they can inflict damage.

### Real Time Threat Prevention

Infinity enables organizations to stay ahead of attackers with real-time threat prevention technologies. Utilizing more than 60 patented threat prevention engines, Infinity blocks attacks across all environments.

- Network-based threat prevention for security gateways with best-in-class IPS, AV, post-infection BOT prevention, sandboxing and malware sanitization.
- Endpoint detection and response with anti-ransomware, AV, post-infection BOT prevention, endpoint sandboxing and forensics
- Advanced mobile threat prevention protects devices from threats to the OS of the device, its apps, and networks
- Infinity's cloud security includes solutions for posture management, native workload protection, public and private network security, visibility and threat hunting, Office 365 email security, branch cloud security and branch virtual security.

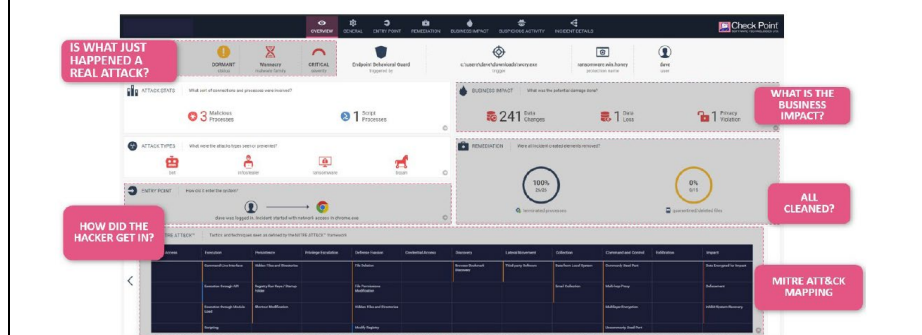
4

<sup>4</sup> <https://www.checkpoint.com/downloads/products/check-point-infinity-datasheet.pdf>

43. Every '441 Accused Product practices receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application, and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components. For example, Check Point Infinity Portal receives process attributes, context information, and behavior information for detected events (sent by Check Point Harmony Endpoint).

NGAV: Runtime Detection and Protection	
Anti-Ransomware	<ul style="list-style-type: none"> <li>Threat Prevention - constantly monitors for ransomware specific behavior and identifies illegitimate file encryption, signature less.</li> <li>Detect and quarantine - All elements of a ransomware attack are identified by forensic analysis and then quarantined.</li> <li>Data Restoration - Encrypted files are automatically restored from snapshots to ensure full business continuity.</li> </ul>
Anti-Exploit	<ul style="list-style-type: none"> <li>Provides protection against exploit based attacks compromising legitimate applications, ensuring those vulnerabilities can't be leveraged.</li> <li>Detects exploits by identifying suspicious memory manipulations in runtime.</li> <li>Shuts down the exploited process upon detecting one, remediates the entire attack chain</li> </ul>
Behavioral Guard	<ul style="list-style-type: none"> <li>Adaptively detects and blocks malware mutations according to their real-time behavior.</li> <li>Identifies, classifies, and blocks malware mutations in real time based on minimal process execution tree similarities.</li> </ul>

**Auto-generated forensic reports:** providing detailed visibility into infected assets, attack flow, correlation with the MITRE ATT&CK™ Framework. The Forensics capability automatically monitors and records endpoint events, including affected files, processes launched, system registry changes, and network activity, and creates a detailed forensic report. Robust attack diagnostics and visibility support remediation efforts, allowing system administrators and incident response teams to effectively triage and resolve attacks.



<sup>5</sup> <https://www.checkpoint.com/downloads/products/harmony-endpoint-solution-brief.pdf>

44. Every '441 Accused Product practices generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result and sending, by the attestation server, the attestation result associated with the application. For example, Check Point Infinity provides automatic forensic reports providing detailed visibility into infected assets including remediation efforts.<sup>6</sup>

45. Defendant has and continues to indirectly infringe one or more claims of the '441 Patent by knowingly and intentionally inducing others, including Check Point subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the '441 Accused Products (*e.g.*, products incorporating the Behavioral Guard with Forensic Reports feature).

46. Defendant, with knowledge that these products, or the use thereof, infringe the '441 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '441 Patent by providing these products to end-users for use in an infringing manner.

47. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '441 Patent, but while remaining willfully blind to the infringement.

48. Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '441 Patent in an amount to be proved at trial.

---

<sup>6</sup> *Id.*

49. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '441 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

**COUNT III**  
**(Infringement of the '038 Patent)**

50. Paragraphs 1 through 27 are incorporated by reference as if fully set forth herein.

51. Neither Taasera Licensing nor TaaSera, Inc. have licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '038 Patent.

52. Defendant has and continues to directly infringe the '038 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '038 Patent. Such products incorporate the compliance and access control features and include at least the Check Point Infinity Portal with Harmony Endpoint (the "'038 Accused Products") which practice a method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software agents on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents; determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and initiating, by the computing system, based on the

compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

53. Every '038 Accused Product practices a method for controlling the operation of an endpoint. For example, Check Point Infinity Portal with Harmony Endpoint performs endpoint threat detection and response.

## CHECK POINT INFINITY

A consolidated cyber security architecture



### INFINITY AT-A-GLANCE

#### Benefits

- Improves security with a consolidated, unified architecture
- Offers real-time threat prevention against known and zero-day threats
- Leverages shared threat intelligence and automation across all enforcement points
- Provides full visibility into organization's threat posture with single, unified management console
- Reduces TCO by 20% and increases operational efficiency by 50%

#### Features

##### Consolidated

Unified protection across the entire IT infrastructure: networks, cloud, endpoints, mobile and IoT devices.

##### Threat Prevention

Uses 64 different threat prevention engines to block against known and zero-day threats, powered by shared threat intelligence.

##### Efficiency

Unified security management, completely automated and seamlessly integrated.

### Changing Business Needs. Rising Threats.

Business needs have changed as most organizations are moving to the Cloud, initiating digital transformation projects, enabling significantly more remote workers, and adding new devices to the network every day. Meanwhile, enterprise security teams are chronically understaffed, working with limited budgets, and using aging tools. Protecting your organization from new, sophisticated cyber attacks has never been more challenging.

Check Point Infinity is the first modern, consolidated, cyber security architecture built to prevent sophisticated Fifth Generation attacks across networks, cloud deployments, endpoints, mobile and IoT devices. Infinity enables organizations to solve security gaps, reduce risk, and lower total cost of ownership.

### Protection for the Entire IT Infrastructure

Infinity enables organizations to prevent cyber threats, simplify security management, and boost efficiency. Infinity's single management console centrally correlates a wide range of events across all network environments, cloud services and mobile infrastructures, with Check Point's pre-emptive threat prevention technologies blocking the most sophisticated attacks before they can inflict damage.

### Real Time Threat Prevention

Infinity enables organizations to stay ahead of attackers with real-time threat prevention technologies. Utilizing more than 60 patented threat prevention engines, Infinity blocks attacks across all environments.

- Network-based threat prevention for security gateways with best-in-class IPS, AV, post-infection BOT prevention, sandboxing and malware sanitization.
- Endpoint detection and response with anti-ransomware, AV, post-infection BOT prevention, endpoint sandboxing and forensics
- Advanced mobile threat prevention protects devices from threats to the OS of the device, its apps, and networks
- Infinity's cloud security includes solutions for posture management, native workload protection, public and private network security, visibility and threat hunting, Office 365 email security, branch cloud security and branch virtual security.

7

<sup>7</sup> <https://www.checkpoint.com/downloads/products/check-point-infinity-datasheet.pdf>

54. Every '038 Accused Product practices providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies and maintaining the plurality of policies in a data store on the computing system. For example, Check Point Infinity allows configuration of a plurality of policies (*e.g.*, Access Control policies) at a system remote from the endpoint through a provided user interface which are stored in a data store.

## Enforcing Access Control

You can enforce access control rules for specific users and groups. It includes three stages:

- Adding users to the policy
- Adding user groups to the policy
- Installing the policy

To get policy enforcement for users and groups:

In the **Policy** menu, click **Access Control**, and then click **Internet Access** to access the policy Rule Base.

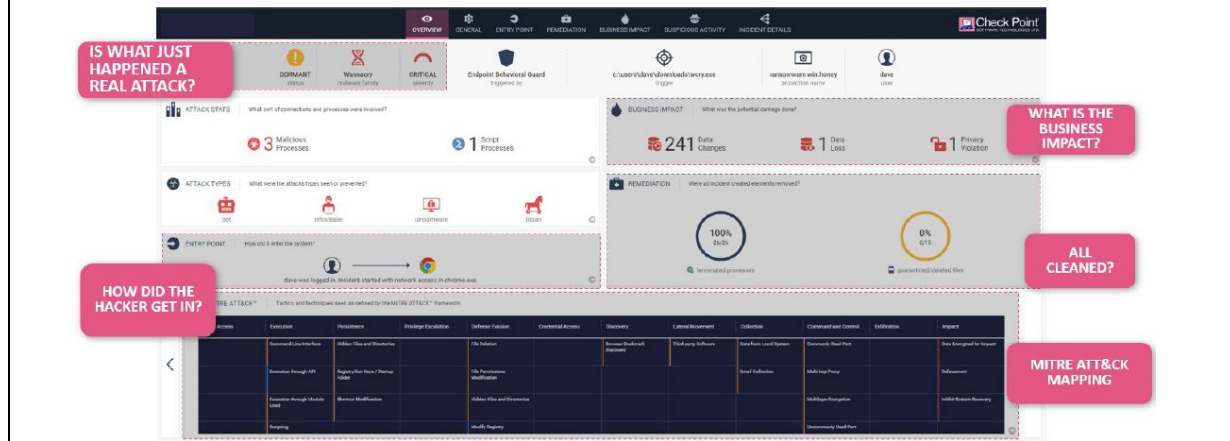
#	Action	Name	Source	Destination
1	Block	Malicious content	* Any Site Or User	Anonymizer, Spyware / Malicious Sites, Botnets, Spam, Phishing, Hacking
2	Block	Explicit content	* Any Site Or User	Violence, Nudity, Pornography, Child Abuse, Gambling, Hate / Racism, Illegal / Questionable, Illegal Drugs, Weapons
3	Block	File sharing	* Any Site Or User	P2P File Sharing
4	Allow	Default rule	* Any Site Or User	Internet

8

55. Every '038 Accused Product practices identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor. For example, Check Point Infinity identifies, from the plurality of policies (*e.g.*, Access Control rules), endpoint events to monitor.

<sup>8</sup> [https://sc1.checkpoint.com/documents/Infinity\\_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce\\_Access\\_Control.htm?Highlight=policy](https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce_Access_Control.htm?Highlight=policy)

**Auto-generated forensic reports:** providing detailed visibility into infected assets, attack flow, correlation with the MITRE ATT&CK™ Framework. The Forensics capability automatically monitors and records endpoint events, including affected files, processes launched, system registry changes, and network activity, and creates a detailed forensic report. Robust attack diagnostics and visibility support remediation efforts, allowing system administrators and incident response teams to effectively triage and resolve attacks.



9

56. Every '038 Accused Product practices configuring one or more software agents on the endpoint to monitor the plurality of operating conditions. For example, Check Point Infinity configures at least the Check Point Harmony Endpoint agent to monitor the plurality of operating conditions (*e.g.*, events and behaviors on the endpoint).<sup>10</sup>


57. Every '038 Accused Product practices receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents. For example, Check Point Infinity receives endpoint events from Check Point Harmony Endpoint agents.<sup>11</sup>

58. Every '038 Accused Product practices determining, by the computing system, a compliance state of the endpoint based on the status information (*e.g.*, detection of endpoint

<sup>9</sup> <https://www.checkpoint.com/downloads/products/harmony-endpoint-solution-brief.pdf>

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*



## CHECK POINT ADVANCED ENDPOINT SECURITY

---

### ADVANCED ENDPOINT SECURITY

**Benefits**

- Protect endpoints from sophisticated attacks and zero-day threats
- Secure data at rest, in use and in transit on endpoint devices
- Reduce security gaps by monitoring, managing, and enforcing user and machine based policies
- Enable deep understanding of security events for faster response endpoint protection
- Defends against multiple attack vectors, including web downloads, external storage devices, lateral movement, or encrypted content
- Single console manages endpoint threat prevention, data security, network access, and compliance

*"A major value with Check Point is centralized control; it gives us a much higher degree of confidence knowing that our entire endpoint is more secure than it's ever been."*

Industry: Government

### OVERVIEW

Unprotected endpoints put an entire business at risk from threats, data loss, and unauthorized access. To mitigate these risks, businesses implement endpoint security, but this can challenge security administrators in multiple ways. Creating and managing new policies for desktops, laptops, Macs, and other devices quickly becomes complicated. In addition, engaging and educating users can take valuable time away from administrators. Different risks and groups require different tools to manage and enforce endpoint and corporate policies. Managing all these aspects requires more of your admin's time, effort, and thinking to execute well.

### SOLUTION

Give your security administrators the power to enforce, manage, report, and educate users under one console. A comprehensive management dashboard gives administrators maximum visibility on security areas important to your organization.

#### ZERO-DAY THREAT PREVENTION

- SandBlast Agent defends endpoints and web browsers with a complete set of real-time advanced browser and endpoint protection technologies, including Threat Emulation, Threat Extraction, Anti-Bot and Zero Phishing.

#### ACTIONABLE INCIDENT ANALYSIS

- SandBlast Agent provides full visibility with its forensics capabilities, monitoring and recording all endpoint events: files affected, processes launched, system registry changes, and network activity.

#### ACCESS CONTROL

- Firewall protects endpoints by controlling inbound and outbound traffic.
- Compliance Check ensures compliance while accessing the corporate network.
- Remote Access VPN secures access to corporate resources when remote.

#### DATA SECURITY

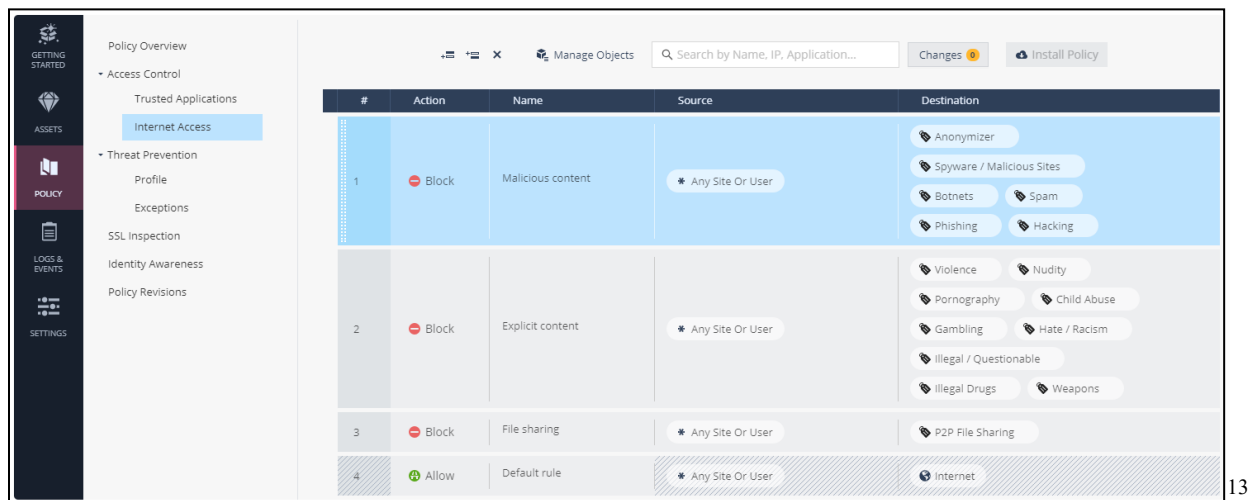
- Full Disk Encryption secures the entire drive.
- Media Encryption encrypts removable storage media.
- Port control enables management and auditing of all endpoint ports.
- Capsule Docs seamlessly protect documents, ensuring access to authorized users.

12

59. Every '038 Accused Product practices initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action

<sup>12</sup> <https://www.checkpoint.com/downloads/products/endpoint-security-datasheet.pdf>

is carried out by a processor on the endpoint. For example, Check Point Infinity Access Control initiates Access Control actions identified in the Access Control rules (*e.g.*, controlling traffic/content to/from the endpoint) based on the compliance state which are carried out by the endpoint processor.



60. Defendant has and continues to indirectly infringe one or more claims of the '038 Patent by knowingly and intentionally inducing others, including Check Point subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the '038 Accused Products (*e.g.*, products incorporating the compliance and access control features).

61. Defendant, with knowledge that these products, or the use thereof, infringe the '038 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '038 Patent by providing these products to end-users for use in an infringing manner.

<sup>13</sup> [https://sc1.checkpoint.com/documents/Infinity\\_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce\\_Access\\_Control.htm?Highlight=policy](https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce_Access_Control.htm?Highlight=policy)

62. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '038 Patent, but while remaining willfully blind to the infringement.

63. Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '038 Patent in an amount to be proved at trial.

64. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '038 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

**COUNT IV**  
**(Infringement of the '948 Patent)**

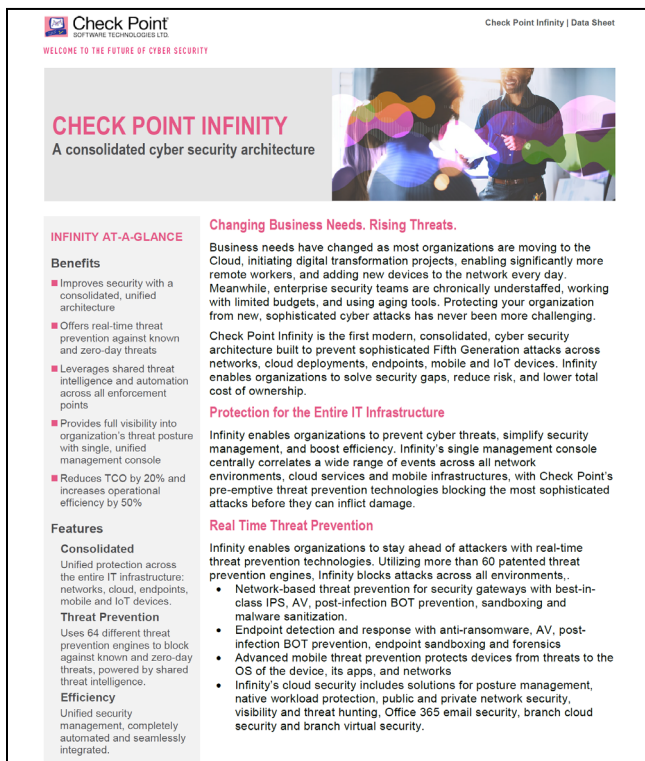
65. Paragraphs 1 through 27 are incorporated by reference as if fully set forth herein.

66. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '948 Patent.

67. Defendant has and continues to directly infringe the '948 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '948 Patent. Such products incorporate the Runtime Detection and Protection and MITRE ATT&CK Framework features and include at least the Check Point Infinity Portal with Harmony Endpoint (the "'948 Accused Products") which practice a method of providing real-time operational integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of

the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor; correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.

68. Every '948 Accused Product practices a method of providing real-time operational integrity of an application on a native computing environment. For example, the Check Point Infinity incorporates real-time threat prevention.



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.  
WELCOME TO THE FUTURE OF CYBER SECURITY

**CHECK POINT INFINITY**  
A consolidated cyber security architecture

**INFINITY AT-A-GLANCE**

**Benefits**

- Improves security with a consolidated, unified architecture
- Offers real-time threat prevention against known and zero-day threats
- Leverages shared threat intelligence and automation across all enforcement points
- Provides full visibility into organization's threat posture with single, unified management console
- Reduces TCO by 20% and increases operational efficiency by 50%

**Features**

**Consolidated**  
Unified protection across the entire IT infrastructure: networks, cloud, endpoints, mobile and IoT devices.

**Threat Prevention**  
Uses 64 different threat prevention engines to block against known and zero-day threats, powered by shared threat intelligence.

**Efficiency**  
Unified security management, completely automated and seamlessly integrated.

**Changing Business Needs. Rising Threats.**  
Business needs have changed as most organizations are moving to the Cloud, initiating digital transformation projects, enabling significantly more remote workers, and adding new devices to the network every day. Meanwhile, enterprise security teams are chronically understaffed, working with limited budgets, and using aging tools. Protecting your organization from new, sophisticated cyber attacks has never been more challenging.

Check Point Infinity is the first modern, consolidated, cyber security architecture built to prevent sophisticated Fifth Generation attacks across networks, cloud deployments, endpoints, mobile and IoT devices. Infinity enables organizations to solve security gaps, reduce risk, and lower total cost of ownership.

**Protection for the Entire IT Infrastructure**  
Infinity enables organizations to prevent cyber threats, simplify security management, and boost efficiency. Infinity's single management console centrally correlates a wide range of events across all network environments, cloud services and mobile infrastructures, with Check Point's pre-emptive threat prevention technologies blocking the most sophisticated attacks before they can inflict damage.

**Real Time Threat Prevention**  
Infinity enables organizations to stay ahead of attackers with real-time threat prevention technologies. Utilizing more than 60 patented threat prevention engines, Infinity blocks attacks across all environments.

- Network-based threat prevention for security gateways with best-in-class IPS, AV, post-infection BOT prevention, sandboxing and malware sanitization.
- Endpoint detection and response with anti-ransomware, AV, post-infection BOT prevention, endpoint sandboxing and forensics
- Advanced mobile threat prevention protects devices from threats to the OS of the device, its apps, and networks
- Infinity's cloud security includes solutions for posture management, native workload protection, public and private network security, visibility and threat hunting, Office 365 email security, branch cloud security and branch virtual security.

14

69. Every '948 Accused Product practices monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application,

<sup>14</sup> <https://www.checkpoint.com/downloads/products/check-point-infinity-datasheet.pdf>

a runtime configuration of the application, resource utilization by the application, and integrity of the application. For example, Check Point Infinity monitors endpoint events and behavior, including affected files, processes launched, system registry changes, and network activity.

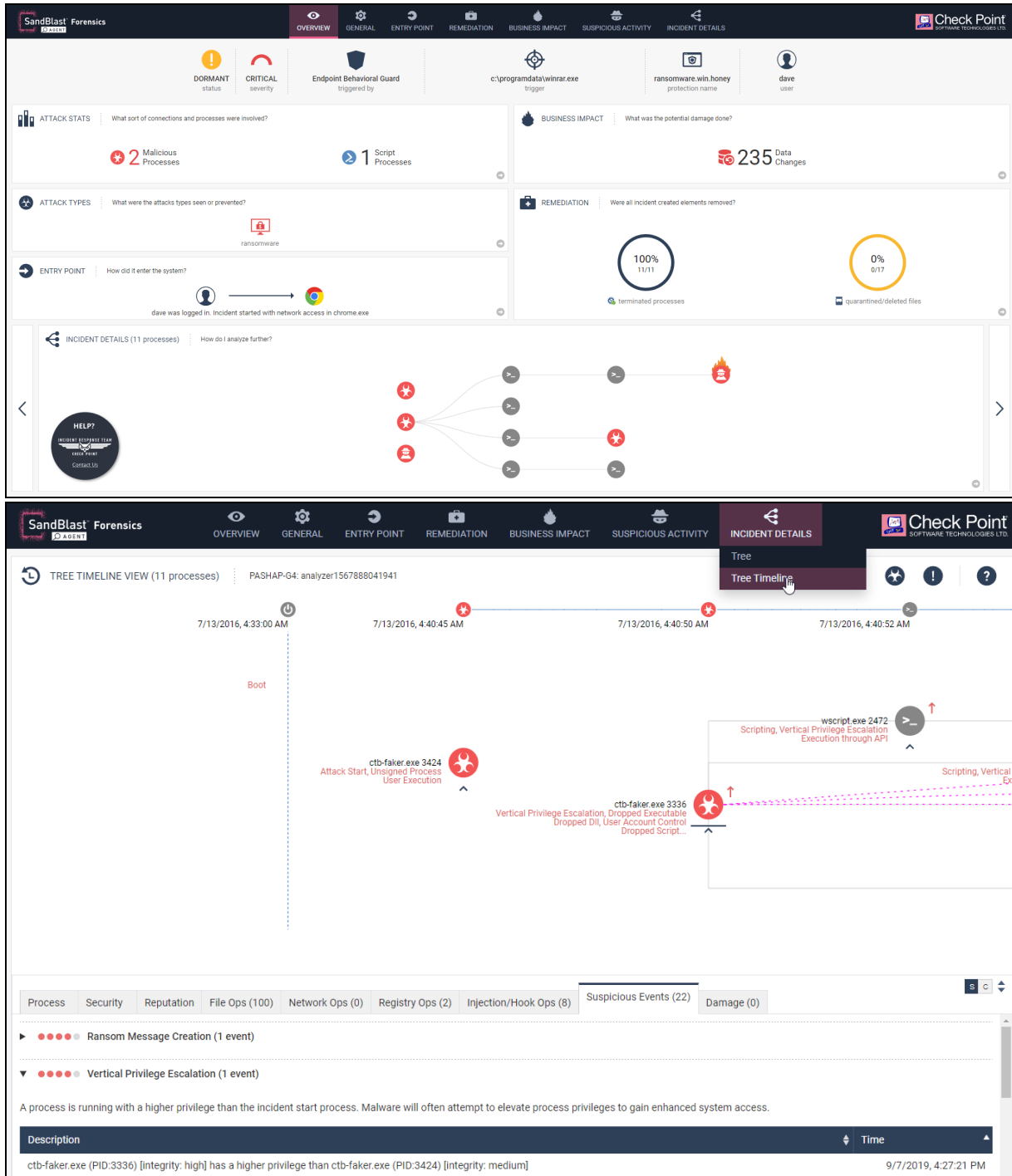
NGAV: Runtime Detection and Protection	
Anti-Ransomware	<ul style="list-style-type: none"> <li>Threat Prevention - constantly monitors for ransomware specific behavior and identifies illegitimate file encryption, signature less.</li> <li>Detect and quarantine - All elements of a ransomware attack are identified by forensic analysis and then quarantined.</li> <li>Data Restoration - Encrypted files are automatically restored from snapshots to ensure full business continuity.</li> </ul>
Anti-Exploit	<ul style="list-style-type: none"> <li>Provides protection against exploit based attacks compromising legitimate applications, ensuring those vulnerabilities can't be leveraged.</li> <li>Detects exploits by identifying suspicious memory manipulations in runtime.</li> <li>Shuts down the exploited process upon detecting one, remediates the entire attack chain</li> </ul>
Behavioral Guard	<ul style="list-style-type: none"> <li>Adaptively detects and blocks malware mutations according to their real-time behavior.</li> <li>Identifies, classifies, and blocks malware mutations in real time based on minimal process execution tree similarities.</li> </ul>

**Auto-generated forensic reports:** providing detailed visibility into infected assets, attack flow, correlation with the MITRE ATT&CK™ Framework. The Forensics capability automatically monitors and records endpoint events, including affected files, processes launched, system registry changes, and network activity, and creates a detailed forensic report. Robust attack diagnostics and visibility support remediation efforts, allowing system administrators and incident response teams to effectively triage and resolve attacks.

15

70. Every '948 Accused Product practices generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor. For example, Check Point Infinity with Harmony Endpoint generates behavior based events for determining the real-time operational integrity of the application executing on the native computer environment.

<sup>15</sup> <https://www.checkpoint.com/downloads/products/harmony-endpoint-solution-brief.pdf>



MITRE ATT&CK™ Matrix | PASHAP-G4: analyzer1567888041941

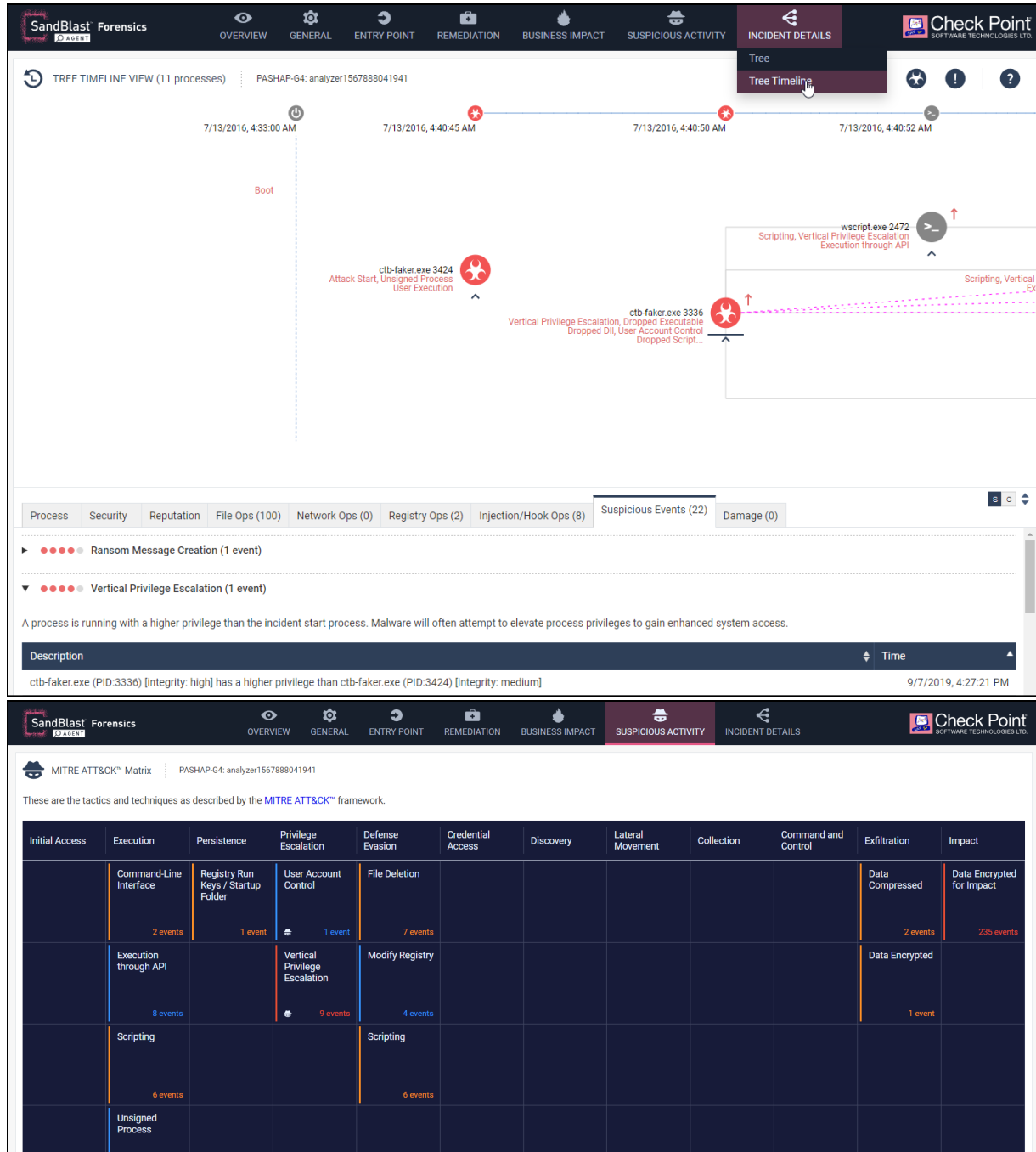
These are the tactics and techniques as described by the MITRE ATT&CK™ framework.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Command-Line Interface 2 events	Registry Run Keys / Startup Folder 1 event	User Account Control 1 event	File Deletion 7 events						Data Compressed 2 events	Data Encrypted for Impact 235 events
	Execution through API 8 events		Vertical Privilege Escalation 9 events	Modify Registry 4 events						Data Encrypted 1 event	
	Scripting 6 events			Scripting 6 events							
	Unsigned Process										

16

71. Every '948 Accused Product practices correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events. For example, the MITRE ATT&CK framework correlates threat classifications based on the temporal sequence of detected behavioral events.

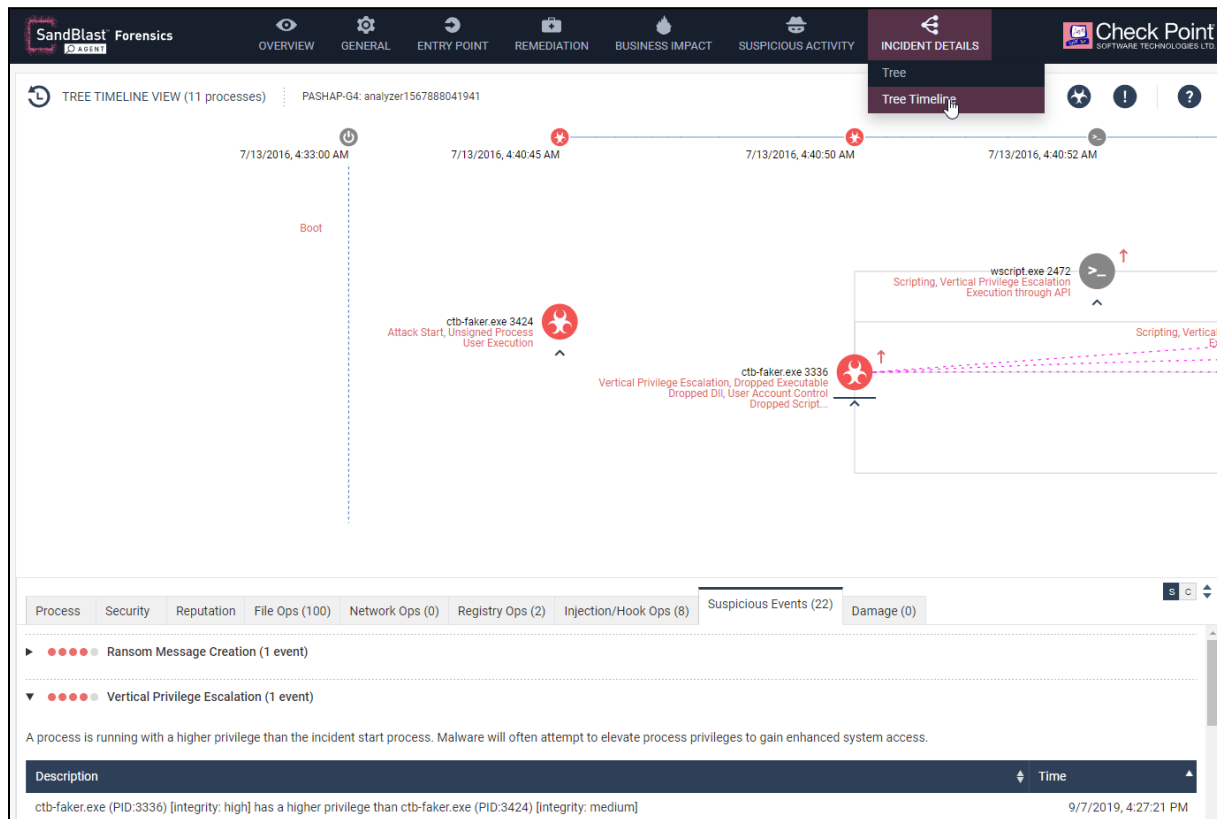
<sup>16</sup> <https://freports.checkpoint.com/ctb-faker/index.html>

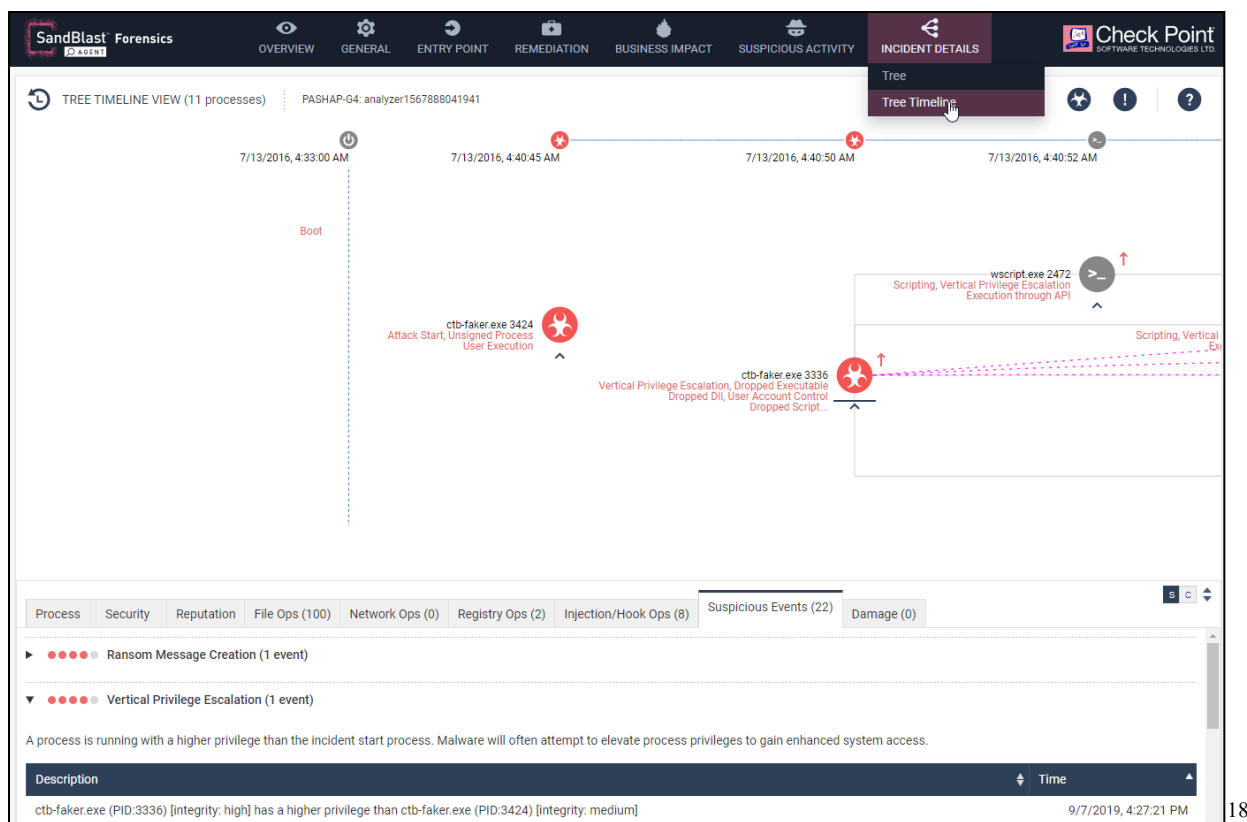


72. Every '948 Accused Product practices displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application. For example, Check Point Infinity includes

<sup>17</sup> *Id.*

several display options for showing real-time status indications for the operational integrity of the application.





18

73. Defendant has and continues to indirectly infringe one or more claims of the '948 Patent by knowingly and intentionally inducing others, including Check Point subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the '948 Accused Products (*e.g.*, products incorporating the Runtime Detection and Protection and MITRE ATT&CK Framework features).

74. Defendant, with knowledge that these products, or the use thereof, infringe the '948 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '948 Patent by providing these products to end-users for use in an infringing manner.

<sup>18</sup> *Id.*

75. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '948 Patent, but while remaining willfully blind to the infringement.

76. Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '948 Patent in an amount to be proved at trial.

77. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '948 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

**COUNT V**  
**(Infringement of the '616 Patent)**

78. Paragraphs 1 through 27 are incorporated by reference as if fully set forth herein.

79. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '616 Patent.

80. Defendant has and continues to directly infringe the '616 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '616 Patent. Such products incorporate the Runtime Detection and Protection and MITRE ATT&CK Framework features and include at least the Check Point Infinity Portal with Harmony Endpoint (the "'616 Accused Products") which practice a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored

device and applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, third-party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments; correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system.

81. Every '616 Accused Product practices a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server. For example, Check Point Infinity comprises Check Point Infinity Portal and Check Point Harmony Endpoint running Sandblast Agent which provides operational integrity of a system.

## CHECK POINT INFINITY

### A consolidated cyber security architecture



#### INFINITY AT-A-GLANCE

##### Benefits

- Improves security with a consolidated, unified architecture
- Offers real-time threat prevention against known and zero-day threats
- Leverages shared threat intelligence and automation across all enforcement points
- Provides full visibility into organization's threat posture with single, unified management console
- Reduces TCO by 20% and increases operational efficiency by 50%

##### Features

###### Consolidated

Unified protection across the entire IT infrastructure: networks, cloud, endpoints, mobile and IoT devices.

###### Threat Prevention

Uses 64 different threat prevention engines to block against known and zero-day threats, powered by shared threat intelligence.

###### Efficiency

Unified security management, completely automated and seamlessly integrated.

#### Changing Business Needs. Rising Threats.

Business needs have changed as most organizations are moving to the Cloud, initiating digital transformation projects, enabling significantly more remote workers, and adding new devices to the network every day. Meanwhile, enterprise security teams are chronically understaffed, working with limited budgets, and using aging tools. Protecting your organization from new, sophisticated cyber attacks has never been more challenging.

Check Point Infinity is the first modern, consolidated, cyber security architecture built to prevent sophisticated Fifth Generation attacks across networks, cloud deployments, endpoints, mobile and IoT devices. Infinity enables organizations to solve security gaps, reduce risk, and lower total cost of ownership.

#### Protection for the Entire IT Infrastructure


Infinity enables organizations to prevent cyber threats, simplify security management, and boost efficiency. Infinity's single management console centrally correlates a wide range of events across all network environments, cloud services and mobile infrastructures, with Check Point's pre-emptive threat prevention technologies blocking the most sophisticated attacks before they can inflict damage.

#### Real Time Threat Prevention

Infinity enables organizations to stay ahead of attackers with real-time threat prevention technologies. Utilizing more than 60 patented threat prevention engines, Infinity blocks attacks across all environments.

- Network-based threat prevention for security gateways with best-in-class IPS, AV, post-infection BOT prevention, sandboxing and malware sanitization.
- Endpoint detection and response with anti-ransomware, AV, post-infection BOT prevention, endpoint sandboxing and forensics
- Advanced mobile threat prevention protects devices from threats to the OS of the device, its apps, and networks
- Infinity's cloud security includes solutions for posture management, native workload protection, public and private network security, visibility and threat hunting, Office 365 email security, branch cloud security and branch virtual security.

<sup>19</sup> <https://www.checkpoint.com/downloads/products/check-point-infinity-datasheet.pdf>





**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

SANDBLAST AGENT DATASHEET

**CHECK POINT**

# SandBlast Agent Endpoint Protection





**CHECK POINT SandBlast Agent Endpoint Protection**

**Advanced Threat Prevention**  
SandBlast Agent prevents and automatically remediates evasive cyberattacks, giving you instant actionable insights of attacks and the protection of user credentials.

**Key Product Benefits**  
Mature endpoint capabilities to

**Cutting-edge threat prevention capabilities**

SandBlast Agent uses a fleet of threat engine technologies to help defend against the full scope of known and unknown zero-day malware. Here are some of the key threat prevention technologies and how they work:

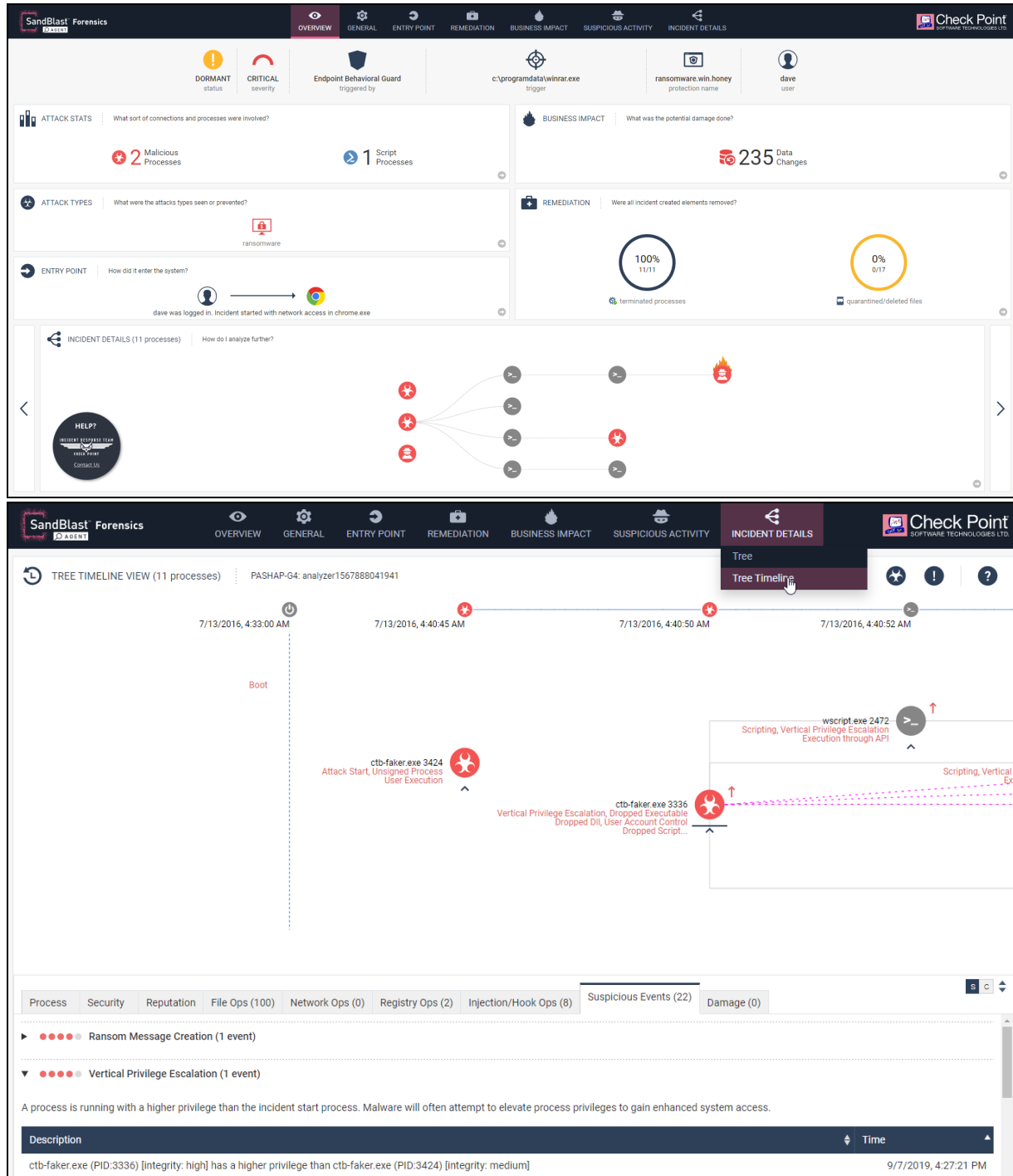
**Threat Emulation / Threat Extraction**  
Every downloaded file using a web browser is put through threat emulation, or a sandboxing process where it is quarantined until deemed safe. Threat extraction ensures users receive “clean” files; the same downloaded file minus dangerous components. The sanitized, risk-free file can then be used normally, plus the option to access the original file.

**Cluster-based forensics**  
Detects and classifies known and unknown malware families based on minimal forensics trees, including:

- Evasion attempts based on malware detection
- Expanding Machine Learning-based context aware detections (for EXEs, file-less script based attacks, and more)
- Baselining behavior of legit apps to detect malicious use of them
- Forensics data behavioral anomaly detection
- Static analysis of EXE for faster detection
- ROP exploit protection
- Attack reputation intelligence
- Expanding Machine Learning-based behavioral models for Behavioral Guard detection logics
- MITRE attack integration into Forensics Records; analyzes endpoint events to provide actionable attack forensics reports

82. Every '616 Accused Product practices sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime. For example, the security agents send events, context, and status information.

<sup>20</sup> <https://www.checkpoint.com/downloads/products/sandblast-agent-datasheet.pdf>

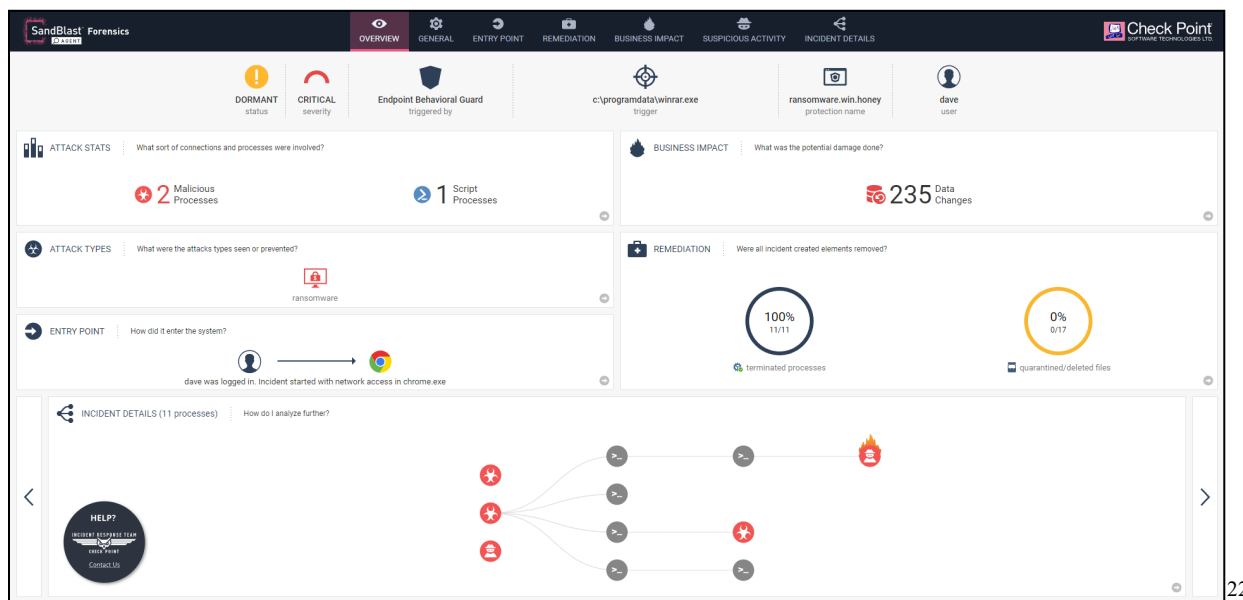


21

83. Every '616 Accused Product practices receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications

<sup>21</sup> <https://freports.checkpoint.com/ctb-faker/index.html>

executing on the monitored device at runtime. For example, Check Point Infinity Portal receives from Endpoint Harmony Sandblast Agent dynamic context including endpoint events and the applications executing on the monitored device in runtime.



22

84. Every '616 Accused Product practices analyzing, by the trust orchestration server, the received endpoint events. For example, Check Point Infinity Portal analyzes endpoint events (*i.e.*, data related to potential security threats).<sup>23</sup>

85. Every '616 Accused Product practices receiving, by the trust orchestration server, third-party network endpoint assessments. For example, Check Point Infinity with Harmony Endpoint and Sandblast Agent receives MITRE ATT&CK data and other third-party network endpoint assessments.

<sup>22</sup> <https://freports.checkpoint.com/ctb-faker/index.html>

<sup>23</sup> *Id.*



**Check Point**  
 SOFTWARE TECHNOLOGIES LTD.

SANDBLAST AGENT DATASHEET

# CHECK POINT

## SandBlast Agent Endpoint Protection





**CHECK POINT SandBlast Agent Endpoint Protection**

**Advanced Threat Prevention**  
SandBlast Agent prevents and automatically remediates evasive cyberattacks, giving you instant actionable insights of attacks and the protection of user credentials.

**Key Product Benefits**  
Mature endpoint capabilities to

### Cutting-edge threat prevention capabilities

SandBlast Agent uses a fleet of threat engine technologies to help defend against the full scope of known and unknown zero-day malware. Here are some of the key threat prevention technologies and how they work:

**Threat Emulation / Threat Extraction**  
Every downloaded file using a web browser is put through threat emulation, or a sandboxing process where it is quarantined until deemed safe. Threat extraction ensures users receive “clean” files; the same downloaded file minus dangerous components. The sanitized, risk-free file can then be used normally, plus the option to access the original file.

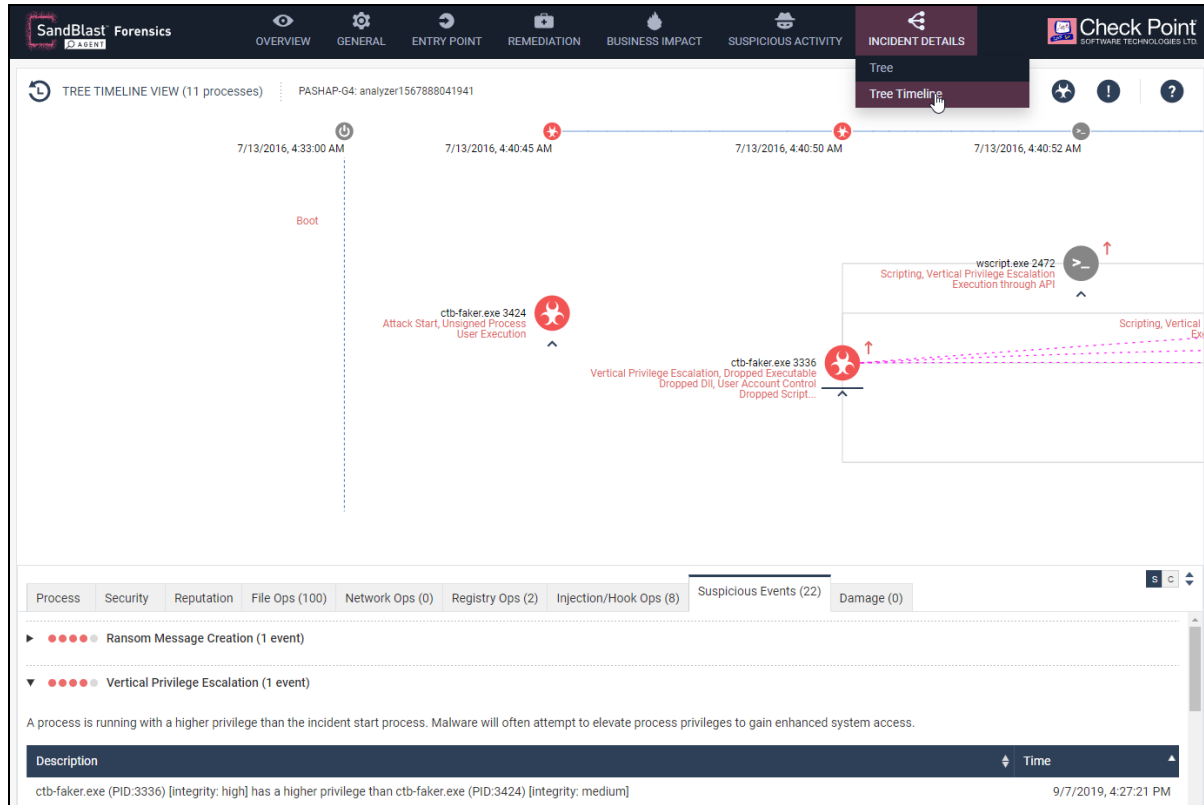
**Cluster-based forensics**  
Detects and classifies known and unknown malware families based on minimal forensics trees, including:

- Evasion attempts based on malware detection
- Expanding Machine Learning-based context aware detections (for EXEs, file-less script based attacks, and more)
- Baselining behavior of legit apps to detect malicious use of them
- Forensics data behavioral anomaly detection
- Static analysis of EXE for faster detection
- ROP exploit protection
- Attack reputation intelligence
- Expanding Machine Learning-based behavioral models for Behavioral Guard detection logics
- MITRE attack integration into Forensics Records; analyzes endpoint events to provide actionable attack forensics reports

24

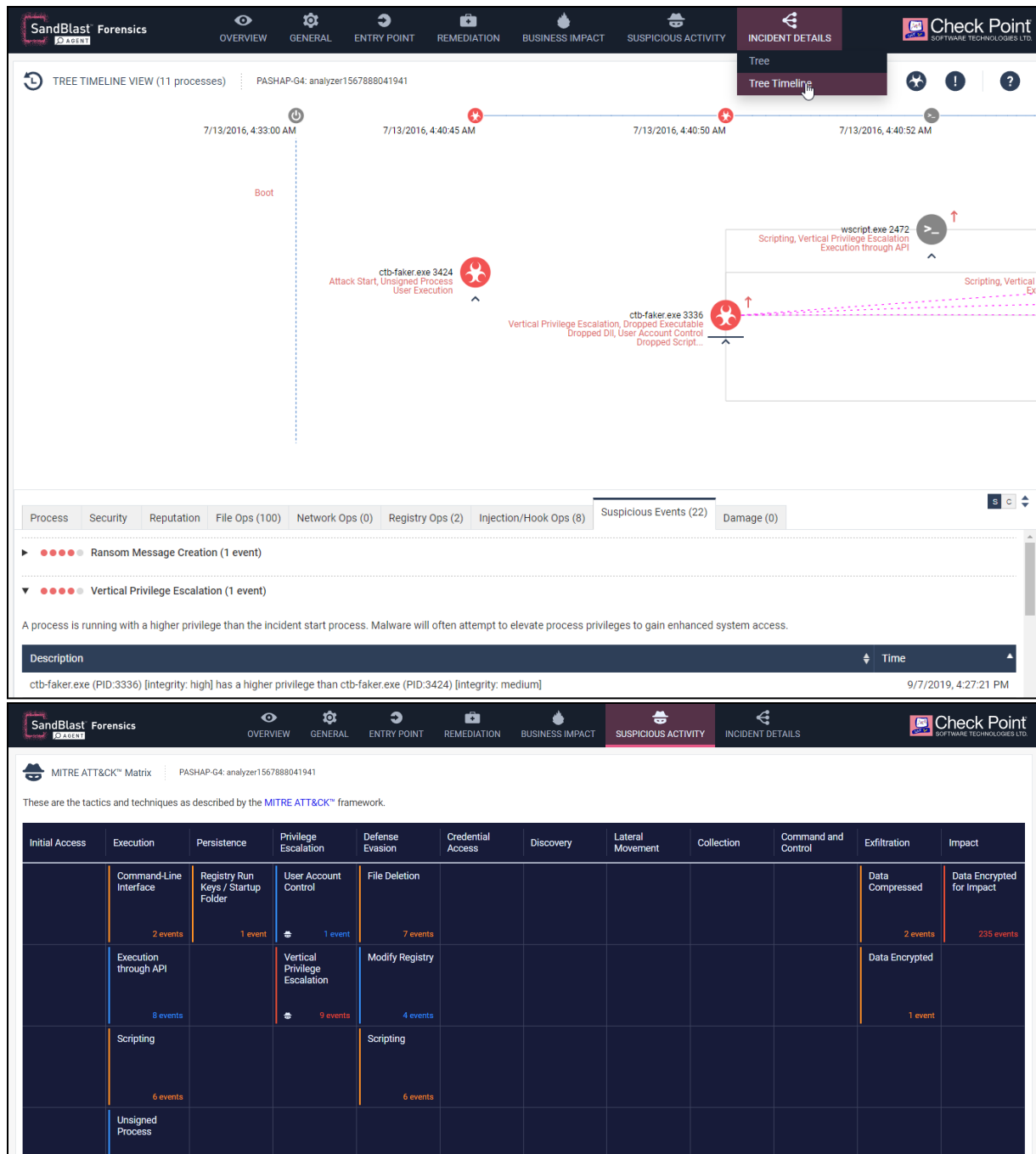
SandBlast Forensics											
OVERVIEW GENERAL ENTRY POINT REMEDIATION BUSINESS IMPACT SUSPICIOUS ACTIVITY INCIDENT DETAILS											
MITRE ATT&CK™ Matrix PASHAP-G4: analyzer156788041941											
These are the tactics and techniques as described by the MITRE ATT&CK™ framework.											
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Command-Line Interface 2 events	Registry Run Keys / Startup Folder 1 event	User Account Control 1 event	File Deletion 7 events						Data Compressed 2 events	Data Encrypted for Impact 235 events
	Execution through API 8 events		Vertical Privilege Escalation 9 events	Modify Registry 4 events						Data Encrypted 1 event	
	Scripting 6 events			Scripting 6 events							
	Unsigned Process										

<sup>24</sup> <https://www.checkpoint.com/downloads/products/sandblast-agent-datasheet.pdf>



86. Every '616 Accused Product practices generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments. For example, Check Point Infinity generates temporal events based at least in part on analyzing the third-party network endpoint assessments (*e.g.*, MITRE ATT&CK tactics and techniques).

<sup>25</sup> <https://freports.checkpoint.com/ctb-faker/index.html>



87. Every '616 Accused Product practices correlating, by the trust orchestration server, the received endpoint events and the generated temporal events. For example, Check Point Infinity

<sup>26</sup> <https://freports.checkpoint.com/ctb-faker/index.html>

correlates the received endpoint events and the generated temporal events (*e.g.*, events correlated to MITRE ATT&CK tactics and techniques).<sup>27</sup>

88. Every '616 Accused Product practices generating, by the trust orchestration server, an integrity profile for the system. For example, Check Point Infinity Smart Event generates an integrity profile for the system.



28

89. Defendant has and continues to indirectly infringe one or more claims of the '616 Patent by knowingly and intentionally inducing others, including Check Point subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that

<sup>27</sup> *Id.*

<sup>28</sup> <https://www.checkpoint.com/downloads/products/smartevent-datasheet.pdf>

include infringing technology, such as '616 Accused Products (*e.g.*, products incorporating the Runtime Detection and Protection and MITRE ATT&CK Framework features).

90. Defendant, with knowledge that these products, or the use thereof, infringe the '616 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '616 Patent by providing these products to end-users for use in an infringing manner.

91. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end- users, infringe the '616 Patent, but while remaining willfully blind to the infringement.

92. Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '616 Patent in an amount to be proved at trial.

93. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '616 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

**COUNT VI**  
**(Infringement of the '997 Patent)**

94. Paragraphs 1 through 27 are incorporated by reference as if fully set forth herein.

95. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '997 Patent.

96. Defendant has and continues to directly infringe the '997 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '997 Patent. Such products incorporate the

compliance and access control features and include at least the Check Point Infinity Portal with Harmony Endpoint (the “’997 Accused Products”) which practice a method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services; determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system.

97. Every ’997 Accused Product practices a method for controlling the operation of an endpoint. For example, Check Point Infinity Portal with Harmony Endpoint performs endpoint threat detection and response.

## CHECK POINT INFINITY

**A consolidated cyber security architecture**



**INFINITY AT-A-GLANCE**

**Benefits**

- Improves security with a consolidated, unified architecture
- Offers real-time threat prevention against known and zero-day threats
- Leverages shared threat intelligence and automation across all enforcement points
- Provides full visibility into organization's threat posture with single, unified management console
- Reduces TCO by 20% and increases operational efficiency by 50%

**Features**

**Consolidated**  
Unified protection across the entire IT infrastructure: networks, cloud, endpoints, mobile and IoT devices.

**Threat Prevention**  
Uses 64 different threat prevention engines to block against known and zero-day threats, powered by shared threat intelligence.

**Efficiency**  
Unified security management, completely automated and seamlessly integrated.

**Changing Business Needs. Rising Threats.**

Business needs have changed as most organizations are moving to the Cloud, initiating digital transformation projects, enabling significantly more remote workers, and adding new devices to the network every day. Meanwhile, enterprise security teams are chronically understaffed, working with limited budgets, and using aging tools. Protecting your organization from new, sophisticated cyber attacks has never been more challenging.

Check Point Infinity is the first modern, consolidated, cyber security architecture built to prevent sophisticated Fifth Generation attacks across networks, cloud deployments, endpoints, mobile and IoT devices. Infinity enables organizations to solve security gaps, reduce risk, and lower total cost of ownership.

**Protection for the Entire IT Infrastructure**

Infinity enables organizations to prevent cyber threats, simplify security management, and boost efficiency. Infinity's single management console centrally correlates a wide range of events across all network environments, cloud services and mobile infrastructures, with Check Point's pre-emptive threat prevention technologies blocking the most sophisticated attacks before they can inflict damage.

**Real Time Threat Prevention**

Infinity enables organizations to stay ahead of attackers with real-time threat prevention technologies. Utilizing more than 60 patented threat prevention engines, Infinity blocks attacks across all environments,.

- Network-based threat prevention for security gateways with best-in-class IPS, AV, post-infection BOT prevention, sandboxing and malware sanitization.
- Endpoint detection and response with anti-ransomware, AV, post-infection BOT prevention, endpoint sandboxing and forensics
- Advanced mobile threat prevention protects devices from threats to the OS of the device, its apps, and networks
- Infinity's cloud security includes solutions for posture management, native workload protection, public and private network security, visibility and threat hunting, Office 365 email security, branch cloud security and branch virtual security.

29

98. Every '997 Accused Product practices providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies and maintaining the plurality of policies in a data store on the computing system. For example, Check

<sup>29</sup> <https://www.checkpoint.com/downloads/products/check-point-infinity-datasheet.pdf>

Point Infinity Portal allows configuration of a plurality of policies (*e.g.*, Access Control rules) at a system remote from the endpoint through a provided user interface which are stored in a data store.

## Enforcing Access Control

You can enforce access control rules for specific users and groups. It includes three stages:

- Adding users to the policy
- Adding user groups to the policy
- Installing the policy

To get policy enforcement for users and groups:

In the **Policy** menu, click **Access Control**, and then click **Internet Access** to access the policy Rule Base.

#	Action	Name	Source	Destination
1	Block	Malicious content	* Any Site Or User	Anonymizer, Spyware / Malicious Sites, Botnets, Spam, Phishing, Hacking
2	Block	Explicit content	* Any Site Or User	Violence, Nudity, Pornography, Child Abuse, Gambling, Hate / Racism, Illegal / Questionable, Illegal Drugs, Weapons
3	Block	File sharing	* Any Site Or User	P2P File Sharing
4	Allow	Default rule	* Any Site Or User	Internet

30

99. Every '997 Accused Product practices identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor. For example, Check Point Infinity Portal identifies, from the plurality of policies (*e.g.*, Access Control rules), events and behaviors on the endpoint to monitor.<sup>31</sup>

100. Every '997 Accused Product practices configuring one or more software services on the endpoint to monitor the plurality of operating conditions. For example, Check Point Infinity

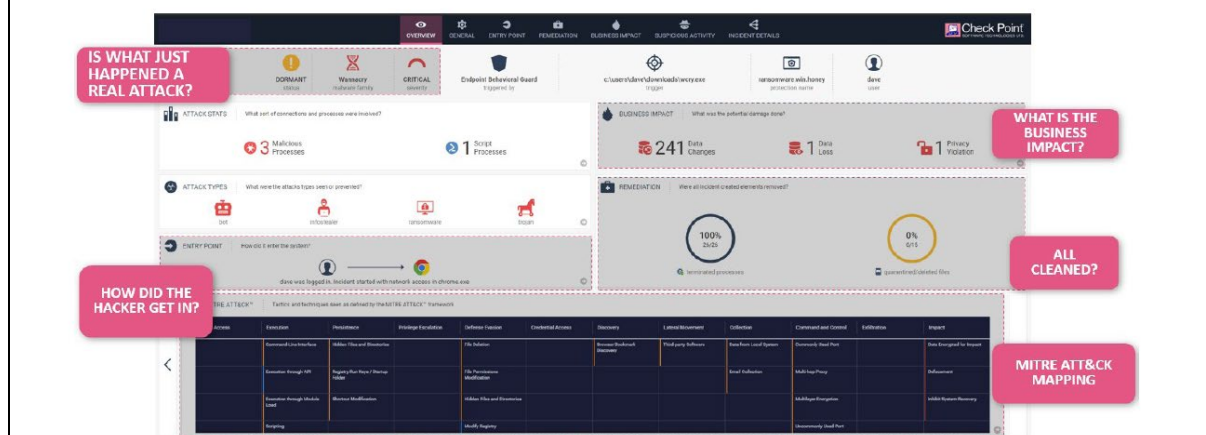
<sup>30</sup> [https://sc1.checkpoint.com/documents/Infinity\\_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce\\_Access\\_Control.htm?Highlight=policy](https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce_Access_Control.htm?Highlight=policy)

<sup>31</sup> *Id.*

Portal configures at least the Access Control module to monitor the plurality of operating conditions (*e.g.*, events and behaviors on the endpoint).

NGAV: Runtime Detection and Protection	
Anti-Ransomware	<ul style="list-style-type: none"> <li>● Threat Prevention - constantly monitors for ransomware specific behavior and identifies illegitimate file encryption, signature less.</li> <li>● Detect and quarantine - All elements of a ransomware attack are identified by forensic analysis and then quarantined.</li> <li>● Data Restoration - Encrypted files are automatically restored from snapshots to ensure full business continuity.</li> </ul>
Anti-Exploit	<ul style="list-style-type: none"> <li>● Provides protection against exploit based attacks compromising legitimate applications, ensuring those vulnerabilities can't be leveraged.</li> <li>● Detects exploits by identifying suspicious memory manipulations in runtime.</li> <li>● Shuts down the exploited process upon detecting one, remediates the entire attack chain</li> </ul>
Behavioral Guard	<ul style="list-style-type: none"> <li>● Adaptively detects and blocks malware mutations according to their real-time behavior.</li> <li>● Identifies, classifies, and blocks malware mutations in real time based on minimal process execution tree similarities.</li> </ul>

**Auto-generated forensic reports:** providing detailed visibility into infected assets, attack flow, correlation with the MITRE ATT&CK™ Framework. The Forensics capability automatically monitors and records endpoint events, including affected files, processes launched, system registry changes, and network activity, and creates a detailed forensic report. Robust attack diagnostics and visibility support remediation efforts, allowing system administrators and incident response teams to effectively triage and resolve attacks.



101. Every '997 Accused Product practices receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services. For example, Infinity Portal receives events and behaviors of the endpoint, gathered by the one or more software services (*e.g.*, Access Control module).<sup>33</sup>

<sup>32</sup> <https://www.checkpoint.com/downloads/products/harmony-endpoint-solution-brief.pdf>

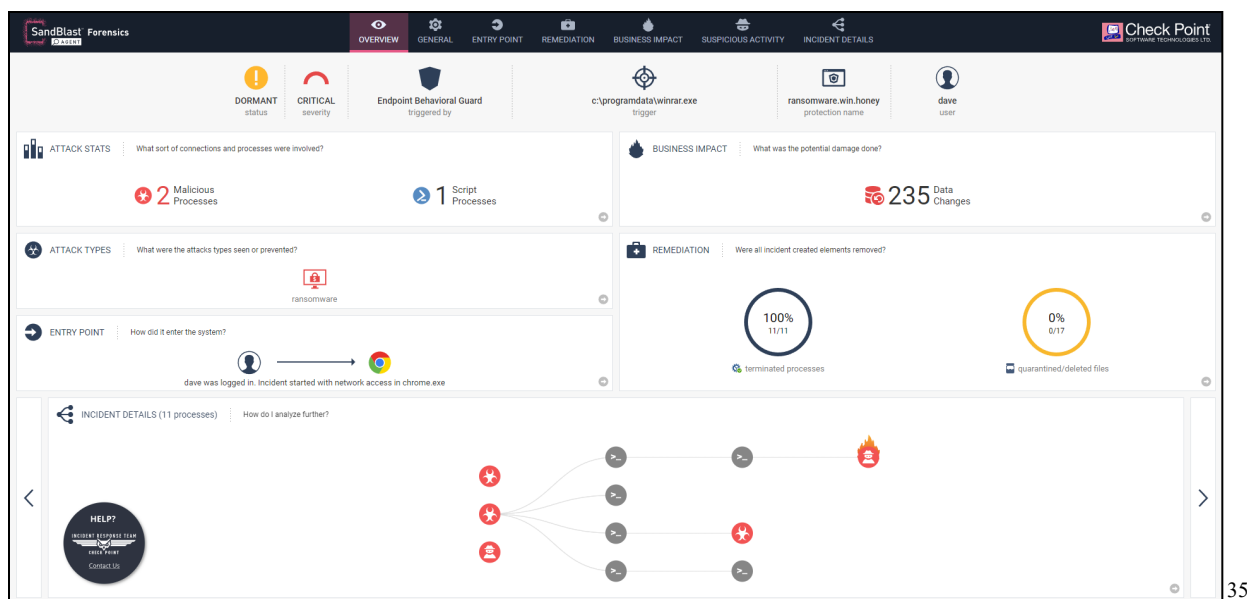
33 *Id.*

102. Every '997 Accused Product practices determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store. For example, Check Point Infinity determines a compliance state of the endpoint based the status information (*e.g.*, detection of endpoint events) and the Access Control rules.

<p><b>ADVANCED ENDPOINT SECURITY</b></p> <p><b>Benefits</b></p> <ul style="list-style-type: none"> <li>• Protect endpoints from sophisticated attacks and zero-day threats</li> <li>• Secure data at rest, in use and in transit on endpoint devices</li> <li>• Reduce security gaps by monitoring, managing, and enforcing user and machine based policies</li> <li>• Enable deep understanding of security events for faster response endpoint protection</li> <li>• Defends against multiple attack vectors, including web downloads, external storage devices, lateral movement, or encrypted content</li> <li>• Single console manages endpoint threat prevention, data security, network access, and compliance</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><i>"A major value with Check Point is centralized control; it gives us a much higher degree of confidence knowing that our entire endpoint is more secure than it's ever been."</i></p> <p>Industry: Government</p> </div>	<p><b>OVERVIEW</b></p> <p>Unprotected endpoints put an entire business at risk from threats, data loss, and unauthorized access. To mitigate these risks, businesses implement endpoint security, but this can challenge security administrators in multiple ways. Creating and managing new policies for desktops, laptops, Macs, and other devices quickly becomes complicated. In addition, engaging and educating users can take valuable time away from administrators. Different risks and groups require different tools to manage and enforce endpoint and corporate policies. Managing all these aspects requires more of your admin's time, effort, and thinking to execute well.</p> <p><b>SOLUTION</b></p> <p>Give your security administrators the power to enforce, manage, report, and educate users under one console. A comprehensive management dashboard gives administrators maximum visibility on security areas important to your organization.</p> <p><b>ZERO-DAY THREAT PREVENTION</b></p> <ul style="list-style-type: none"> <li>• SandBlast Agent defends endpoints and web browsers with a complete set of real-time advanced browser and endpoint protection technologies, including Threat Emulation, Threat Extraction, Anti-Bot and Zero Phishing.</li> </ul> <p><b>ACTIONABLE INCIDENT ANALYSIS</b></p> <ul style="list-style-type: none"> <li>• SandBlast Agent provides full visibility with its forensics capabilities, monitoring and recording all endpoint events: files affected, processes launched, system registry changes, and network activity.</li> </ul> <p><b>ACCESS CONTROL</b></p> <ul style="list-style-type: none"> <li>• Firewall protects endpoints by controlling inbound and outbound traffic.</li> <li>• Compliance Check ensures compliance while accessing the corporate network.</li> <li>• Remote Access VPN secures access to corporate resources when remote.</li> </ul> <p><b>DATA SECURITY</b></p> <ul style="list-style-type: none"> <li>• Full Disk Encryption secures the entire drive.</li> <li>• Media Encryption encrypts removable storage media.</li> <li>• Port control enables management and auditing of all endpoint ports.</li> <li>• Capsule Docs seamlessly protect documents, ensuring access to authorized users.</li> </ul>
---	---

34

<sup>34</sup> <https://www.checkpoint.com/downloads/products/endpoint-security-datasheet.pdf>



35

103. Every '997 Accused Product practices initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system. For example, Check Point Infinity remotely initiates actions identified in the Access Control rules (*e.g.*, controlling traffic/content to/from the endpoint) based on the compliance state that are carried out by the endpoint processor.

<sup>35</sup> <https://freports.checkpoint.com/ctb-faker/index.html>

<h2 style="color: #e91e63;">ADVANCED ENDPOINT SECURITY</h2> <p><b>Benefits</b></p> <ul style="list-style-type: none"> <li>• Protect endpoints from sophisticated attacks and zero-day threats</li> <li>• Secure data at rest, in use and in transit on endpoint devices</li> <li>• Reduce security gaps by monitoring, managing, and enforcing user and machine based policies</li> <li>• Enable deep understanding of security events for faster response endpoint protection</li> <li>• Defends against multiple attack vectors, including web downloads, external storage devices, lateral movement, or encrypted content</li> <li>• Single console manages endpoint threat prevention, data security, network access, and compliance</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><i>"A major value with Check Point is centralized control; it gives us a much higher degree of confidence knowing that our entire endpoint is more secure than it's ever been."</i></p> <p>Industry: Government</p> </div>	<h2 style="color: #e91e63;">OVERVIEW</h2> <p>Unprotected endpoints put an entire business at risk from threats, data loss, and unauthorized access. To mitigate these risks, businesses implement endpoint security, but this can challenge security administrators in multiple ways. Creating and managing new policies for desktops, laptops, Macs, and other devices quickly becomes complicated. In addition, engaging and educating users can take valuable time away from administrators. Different risks and groups require different tools to manage and enforce endpoint and corporate policies. Managing all these aspects requires more of your admin's time, effort, and thinking to execute well.</p> <h2 style="color: #e91e63;">SOLUTION</h2> <p>Give your security administrators the power to enforce, manage, report, and educate users under one console. A comprehensive management dashboard gives administrators maximum visibility on security areas important to your organization.</p> <h3 style="background-color: #424242; color: white; padding: 2px;">ZERO-DAY THREAT PREVENTION</h3> <ul style="list-style-type: none"> <li>• SandBlast Agent defends endpoints and web browsers with a complete set of real-time advanced browser and endpoint protection technologies, including Threat Emulation, Threat Extraction, Anti-Bot and Zero Phishing.</li> </ul> <h3 style="background-color: #424242; color: white; padding: 2px;">ACTIONABLE INCIDENT ANALYSIS</h3> <ul style="list-style-type: none"> <li>• SandBlast Agent provides full visibility with its forensics capabilities, monitoring and recording all endpoint events: files affected, processes launched, system registry changes, and network activity.</li> </ul> <h3 style="background-color: #424242; color: white; padding: 2px;">ACCESS CONTROL</h3> <ul style="list-style-type: none"> <li>• Firewall protects endpoints by controlling inbound and outbound traffic.</li> <li>• Compliance Check ensures compliance while accessing the corporate network.</li> <li>• Remote Access VPN secures access to corporate resources when remote.</li> </ul> <h3 style="background-color: #424242; color: white; padding: 2px;">DATA SECURITY</h3> <ul style="list-style-type: none"> <li>• Full Disk Encryption secures the entire drive.</li> <li>• Media Encryption encrypts removable storage media.</li> <li>• Port control enables management and auditing of all endpoint ports.</li> <li>• Capsule Docs seamlessly protect documents, ensuring access to authorized users.</li> </ul>
--	---

36

104. Defendant has and continues to indirectly infringe one or more claims of the '997 Patent by knowingly and intentionally inducing others, including Check Point subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the '997 Accused Products (*e.g.*, compliance and access control features).

105. Defendant, with knowledge that these products, or the use thereof, infringe the '997 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues

<sup>36</sup> <https://www.checkpoint.com/downloads/products/endpoint-security-datasheet.pdf>

to knowingly and intentionally induce, direct infringement of the '997 Patent by providing these products to end-users for use in an infringing manner.

106. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '997 Patent, but while remaining willfully blind to the infringement.

107. Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '997 Patent in an amount to be proved at trial.

108. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '997 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

**COUNT VII**  
**(Infringement of the '918 Patent)**

109. Paragraphs 1 through 27 are incorporated by reference as if fully set forth herein.

110. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '918 Patent.


111. Defendant has and continues to directly infringe the '918 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '918 Patent. Such products incorporate the compliance and access control features and include at least the Check Point Infinity Portal with Harmony Endpoint (the "'918 Accused Products") which comprise a system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; a data store, at the

computing system, that contains the plurality of policies; one or more software services, provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to receive, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint, determine, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store, and authorize access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state.

112. Every '918 Accused Product comprises a system for controlling the operation of an endpoint. For example, Check Point Infinity Portal with Harmony Endpoint performs endpoint threat detection and response.

## CHECK POINT INFINITY

**A consolidated cyber security architecture**



**INFINITY AT-A-GLANCE**

**Benefits**

- Improves security with a consolidated, unified architecture
- Offers real-time threat prevention against known and zero-day threats
- Leverages shared threat intelligence and automation across all enforcement points
- Provides full visibility into organization's threat posture with single, unified management console
- Reduces TCO by 20% and increases operational efficiency by 50%

**Features**

**Consolidated**  
Unified protection across the entire IT infrastructure: networks, cloud, endpoints, mobile and IoT devices.

**Threat Prevention**  
Uses 64 different threat prevention engines to block against known and zero-day threats, powered by shared threat intelligence.

**Efficiency**  
Unified security management, completely automated and seamlessly integrated.

**Changing Business Needs. Rising Threats.**

Business needs have changed as most organizations are moving to the Cloud, initiating digital transformation projects, enabling significantly more remote workers, and adding new devices to the network every day. Meanwhile, enterprise security teams are chronically understaffed, working with limited budgets, and using aging tools. Protecting your organization from new, sophisticated cyber attacks has never been more challenging.

Check Point Infinity is the first modern, consolidated, cyber security architecture built to prevent sophisticated Fifth Generation attacks across networks, cloud deployments, endpoints, mobile and IoT devices. Infinity enables organizations to solve security gaps, reduce risk, and lower total cost of ownership.

**Protection for the Entire IT Infrastructure**

Infinity enables organizations to prevent cyber threats, simplify security management, and boost efficiency. Infinity's single management console centrally correlates a wide range of events across all network environments, cloud services and mobile infrastructures, with Check Point's pre-emptive threat prevention technologies blocking the most sophisticated attacks before they can inflict damage.

**Real Time Threat Prevention**

Infinity enables organizations to stay ahead of attackers with real-time threat prevention technologies. Utilizing more than 60 patented threat prevention engines, Infinity blocks attacks across all environments,.

- Network-based threat prevention for security gateways with best-in-class IPS, AV, post-infection BOT prevention, sandboxing and malware sanitization.
- Endpoint detection and response with anti-ransomware, AV, post-infection BOT prevention, endpoint sandboxing and forensics
- Advanced mobile threat prevention protects devices from threats to the OS of the device, its apps, and networks
- Infinity's cloud security includes solutions for posture management, native workload protection, public and private network security, visibility and threat hunting, Office 365 email security, branch cloud security and branch virtual security.

37

113. Every '918 Accused Product comprises a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies, and a data store, at the computing system, that contains the plurality of policies. For example, Check Point Infinity Portal comprises a user interface that allows configuration of a plurality of policies

<sup>37</sup> <https://www.checkpoint.com/downloads/products/check-point-infinity-datasheet.pdf>

(e.g., Access Control rules) at a system remote from the endpoint which are stored in the Infinity Portal.

## Enforcing Access Control

You can enforce access control rules for specific users and groups. It includes three stages:

- Adding users to the policy
- Adding user groups to the policy
- Installing the policy

To get policy enforcement for users and groups:

In the **Policy** menu, click **Access Control**, and then click **Internet Access** to access the policy Rule Base.

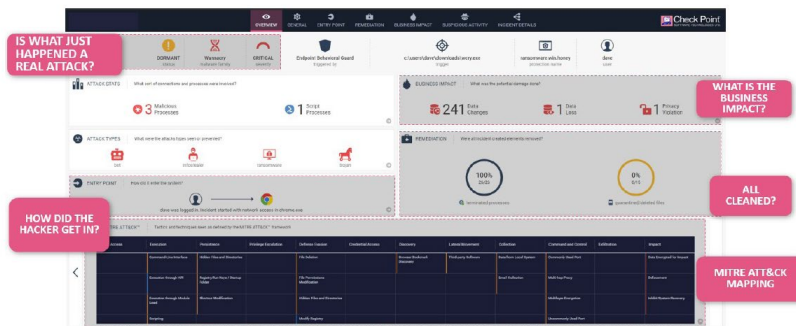
#	Action	Name	Source	Destination
1	Block	Malicious content	* Any Site Or User	Anonymizer, Spyware / Malicious Sites, Botnets, Spam, Phishing, Hacking
2	Block	Explicit content	* Any Site Or User	Violence, Nudity, Pornography, Child Abuse, Gambling, Hate / Racism, Illegal / Questionable, Illegal Drugs, Weapons
3	Block	File sharing	* Any Site Or User	P2P File Sharing
4	Allow	Default rule	* Any Site Or User	Internet

114. Every '918 Accused Product comprises one or more software services, provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies. For example, at least the Check Point Harmony Endpoint with Sandblast Agent is configured to evaluate the plurality of operating conditions (e.g., events and behaviors on the endpoint) identified in the plurality of policies (e.g., Access Control rules).

<sup>38</sup> [https://sc1.checkpoint.com/documents/Infinity\\_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce\\_Access\\_Control.htm?Highlight=policy](https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce_Access_Control.htm?Highlight=policy)

NGAV: Runtime Detection and Protection	
Anti-Ransomware	<ul style="list-style-type: none"> <li>Threat Prevention - constantly monitors for ransomware specific behavior and identifies illegitimate file encryption, signature less.</li> <li>Detect and quarantine - All elements of a ransomware attack are identified by forensic analysis and then quarantined.</li> <li>Data Restoration - Encrypted files are automatically restored from snapshots to ensure full business continuity.</li> </ul>
Anti-Exploit	<ul style="list-style-type: none"> <li>Provides protection against exploit based attacks compromising legitimate applications, ensuring those vulnerabilities can't be leveraged.</li> <li>Detects exploits by identifying suspicious memory manipulations in runtime.</li> <li>Shuts down the exploited process upon detecting one, remediates the entire attack chain</li> </ul>
Behavioral Guard	<ul style="list-style-type: none"> <li>Adaptively detects and blocks malware mutations according to their real-time behavior.</li> <li>Identifies, classifies, and blocks malware mutations in real time based on minimal process execution tree similarities.</li> </ul>

**Auto-generated forensic reports:** providing detailed visibility into infected assets, attack flow, correlation with the MITRE ATT&CK™ Framework. The Forensics capability automatically monitors and records endpoint events, including affected files, processes launched, system registry changes, and network activity, and creates a detailed forensic report. Robust attack diagnostics and visibility support remediation efforts, allowing system administrators and incident response teams to effectively triage and resolve attacks.



39

## Enforcing Access Control

You can enforce access control rules for specific users and groups. It includes three stages:

- Adding users to the policy
- Adding user groups to the policy
- Installing the policy

To get policy enforcement for users and groups:

In the **Policy** menu, click **Access Control**, and then click **Internet Access** to access the policy Rule Base.

#	Action	Name	Source	Destination
1	Block	Malicious content	Any Site Or User	Any Site Or User
2	Block	Explicit content	Any Site Or User	Any Site Or User
3	Block	File sharing	Any Site Or User	Any Site Or User
4	Allow	Default rule	Any Site Or User	Internet

40

<sup>39</sup> <https://www.checkpoint.com/downloads/products/harmony-endpoint-solution-brief.pdf>

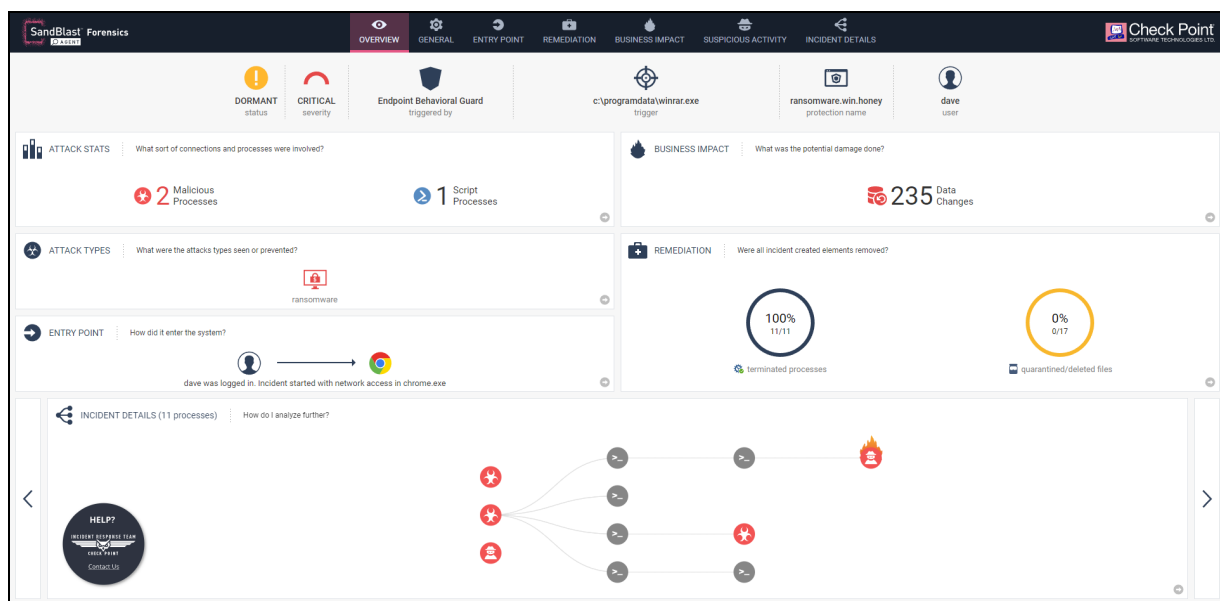
<sup>40</sup> [https://sc1.checkpoint.com/documents/Infinity\\_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce\\_Access\\_Control.htm?Highlight=policy](https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce_Access_Control.htm?Highlight=policy)

115. Every '918 Accused Product receives, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services on the endpoint, and user information that identified a user of the endpoint. For example, Check Point Infinity Portal receives endpoint events and behavior alerts gathered by the one or more software services (*e.g.*, Access Control module), and identification of a user of the endpoint.

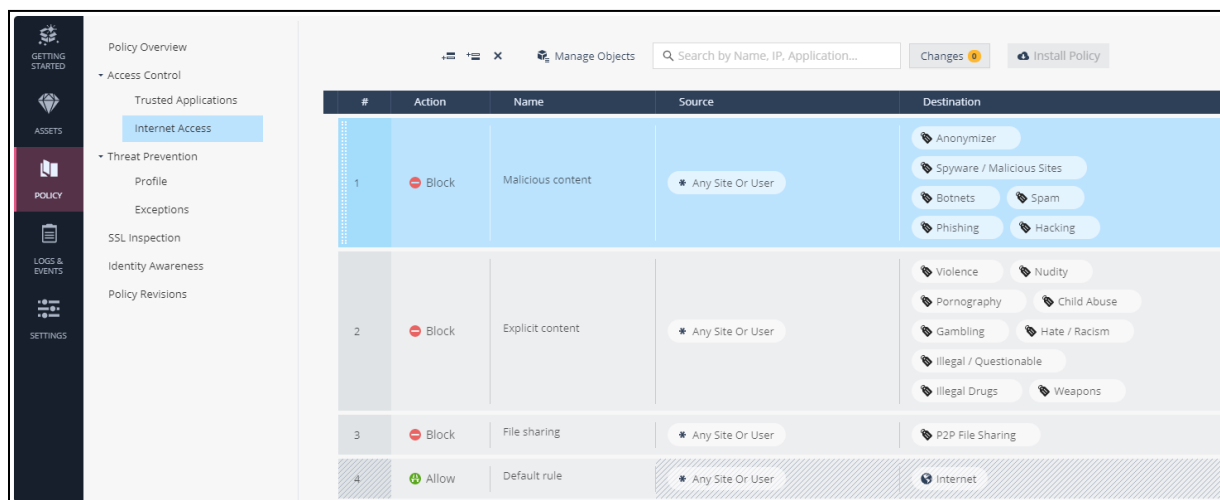
<h2>ADVANCED ENDPOINT SECURITY</h2> <p><b>Benefits</b></p> <ul style="list-style-type: none"> <li>• Protect endpoints from sophisticated attacks and zero-day threats</li> <li>• Secure data at rest, in use and in transit on endpoint devices</li> <li>• Reduce security gaps by monitoring, managing, and enforcing user and machine based policies</li> <li>• Enable deep understanding of security events for faster response endpoint protection</li> <li>• Defends against multiple attack vectors, including web downloads, external storage devices, lateral movement, or encrypted content</li> <li>• Single console manages endpoint threat prevention, data security, network access, and compliance</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><i>"A major value with Check Point is centralized control; it gives us a much higher degree of confidence knowing that our entire endpoint is more secure than it's ever been."</i></p> <p>Industry: Government</p> </div>	<h2>OVERVIEW</h2> <p>Unprotected endpoints put an entire business at risk from threats, data loss, and unauthorized access. To mitigate these risks, businesses implement endpoint security, but this can challenge security administrators in multiple ways. Creating and managing new policies for desktops, laptops, Macs, and other devices quickly becomes complicated. In addition, engaging and educating users can take valuable time away from administrators. Different risks and groups require different tools to manage and enforce endpoint and corporate policies. Managing all these aspects requires more of your admin's time, effort, and thinking to execute well.</p> <h2>SOLUTION</h2> <p>Give your security administrators the power to enforce, manage, report, and educate users under one console. A comprehensive management dashboard gives administrators maximum visibility on security areas important to your organization.</p> <h3>ZERO-DAY THREAT PREVENTION</h3> <ul style="list-style-type: none"> <li>• SandBlast Agent defends endpoints and web browsers with a complete set of real-time advanced browser and endpoint protection technologies, including Threat Emulation, Threat Extraction, Anti-Bot and Zero Phishing.</li> </ul> <h3>ACTIONABLE INCIDENT ANALYSIS</h3> <ul style="list-style-type: none"> <li>• SandBlast Agent provides full visibility with its forensics capabilities, monitoring and recording all endpoint events: files affected, processes launched, system registry changes, and network activity.</li> </ul> <h3>ACCESS CONTROL</h3> <ul style="list-style-type: none"> <li>• Firewall protects endpoints by controlling inbound and outbound traffic.</li> <li>• Compliance Check ensures compliance while accessing the corporate network.</li> <li>• Remote Access VPN secures access to corporate resources when remote.</li> </ul> <h3>DATA SECURITY</h3> <ul style="list-style-type: none"> <li>• Full Disk Encryption secures the entire drive.</li> <li>• Media Encryption encrypts removable storage media.</li> <li>• Port control enables management and auditing of all endpoint ports.</li> <li>• Capsule Docs seamlessly protect documents, ensuring access to authorized users.</li> </ul>
--	---

41

<sup>41</sup> <https://www.checkpoint.com/downloads/products/endpoint-security-datasheet.pdf>



42

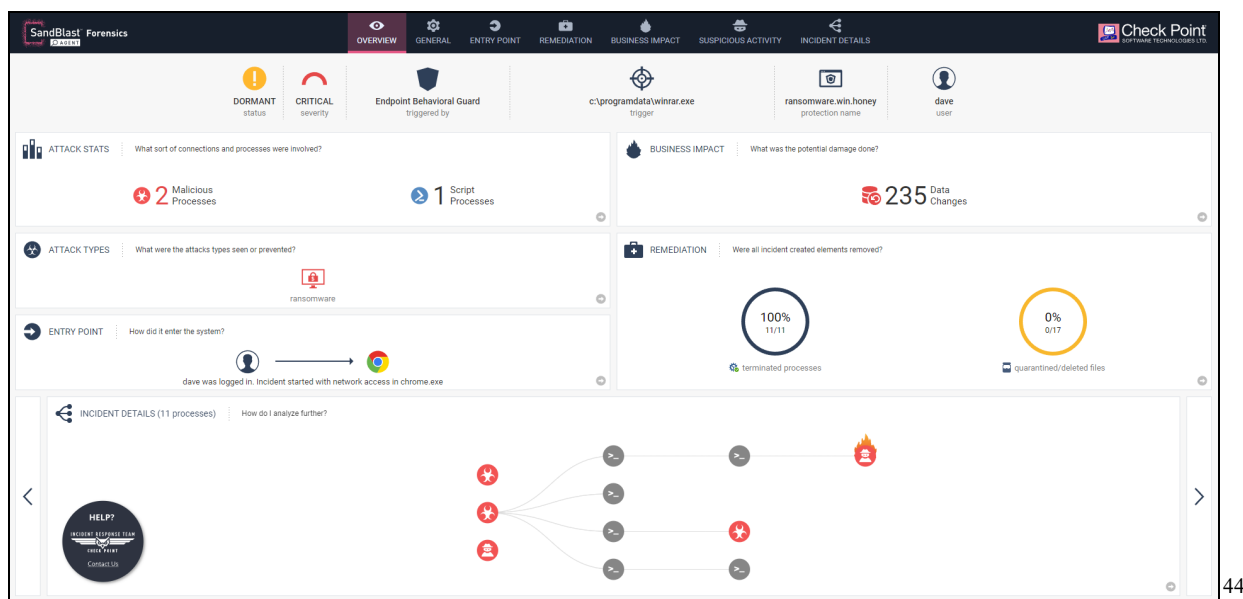


43

116. Every '918 Accused Product determines, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store. For example, Check Point Infinity determines a compliance state of the endpoint based on the user information, endpoint events, behavior alerts, and the Access Control rules.

<sup>42</sup> <https://freports.checkpoint.com/ctb-faker/index.html>

<sup>43</sup> [https://sc1.checkpoint.com/documents/Infinity\\_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce\\_Access\\_Control.htm?Highlight=policy](https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce_Access_Control.htm?Highlight=policy)



44

117. Every '918 Accused Product authorizes access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state. For example, Check Point Infinity Access Control authorizes access by the endpoint to a computing resource on the network (*e.g.*, controlling traffic/content to/from the endpoint), authorization being determined by Check Point Infinity in response to the compliance state.

<sup>44</sup> <https://freports.checkpoint.com/ctb-faker/index.html>



# CHECK POINT ADVANCED ENDPOINT SECURITY

## ADVANCED ENDPOINT SECURITY

### Benefits

- Protect endpoints from sophisticated attacks and zero-day threats
- Secure data at rest, in use and in transit on endpoint devices
- Reduce security gaps by monitoring, managing, and enforcing user and machine based policies
- Enable deep understanding of security events for faster response endpoint protection
- Defends against multiple attack vectors, including web downloads, external storage devices, lateral movement, or encrypted content
- Single console manages endpoint threat prevention, data security, network access, and compliance

*"A major value with Check Point is centralized control; it gives us a much higher degree of confidence knowing that our entire endpoint is more secure than it's ever been."*

Industry: Government

### OVERVIEW

Unprotected endpoints put an entire business at risk from threats, data loss, and unauthorized access. To mitigate these risks, businesses implement endpoint security, but this can challenge security administrators in multiple ways. Creating and managing new policies for desktops, laptops, Macs, and other devices quickly becomes complicated. In addition, engaging and educating users can take valuable time away from administrators. Different risks and groups require different tools to manage and enforce endpoint and corporate policies. Managing all these aspects requires more of your admin's time, effort, and thinking to execute well.

### SOLUTION

Give your security administrators the power to enforce, manage, report, and educate users under one console. A comprehensive management dashboard gives administrators maximum visibility on security areas important to your organization.

#### ZERO-DAY THREAT PREVENTION

- SandBlast Agent defends endpoints and web browsers with a complete set of real-time advanced browser and endpoint protection technologies, including Threat Emulation, Threat Extraction, Anti-Bot and Zero Phishing.

#### ACTIONABLE INCIDENT ANALYSIS

- SandBlast Agent provides full visibility with its forensics capabilities, monitoring and recording all endpoint events: files affected, processes launched, system registry changes, and network activity.

#### ACCESS CONTROL

- Firewall protects endpoints by controlling inbound and outbound traffic.
- Compliance Check ensures compliance while accessing the corporate network.
- Remote Access VPN secures access to corporate resources when remote.

#### DATA SECURITY

- Full Disk Encryption secures the entire drive.
- Media Encryption encrypts removable storage media.
- Port control enables management and auditing of all endpoint ports.
- Capsule Docs seamlessly protect documents, ensuring access to authorized users.

45

<sup>45</sup> <https://www.checkpoint.com/downloads/products/endpoint-security-datasheet.pdf>

# Enforcing Access Control

You can enforce access control rules for specific users and groups. It includes three stages:

- Adding users to the policy
- Adding user groups to the policy
- Installing the policy

To get policy enforcement for users and groups:

In the **Policy** menu, click **Access Control**, and then click **Internet Access** to access the policy Rule Base.

#	Action	Name	Source	Destination
1	Block	Malicious content	* Any Site Or User	Anonymizer, Spyware / Malicious Sites, Botnets, Spam, Phishing, Hacking
2	Block	Explicit content	* Any Site Or User	Violence, Nudity, Pornography, Child Abuse, Gambling, Hate / Racism, Illegal / Questionable, Illegal Drugs, Weapons
3	Block	File sharing	* Any Site Or User	P2P File Sharing
4	Allow	Default rule	* Any Site Or User	Internet

46

118. Defendant has and continues to indirectly infringe one or more claims of the '918 Patent by knowingly and intentionally inducing others, including Check Point subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the '918 Accused Products (*e.g.*, products incorporating the compliance and access control features).

119. Defendant, with knowledge that these products, or the use thereof, infringe the '918 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues

<sup>46</sup> [https://sc1.checkpoint.com/documents/Infinity\\_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce\\_Access\\_Control.htm?Highlight=policy](https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Topics-Harmony-Connect-AG/Policy/Enforce_Access_Control.htm?Highlight=policy)

to knowingly and intentionally induce, direct infringement of the '918 Patent by providing these products to end-users for use in an infringing manner.

120. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '918 Patent, but while remaining willfully blind to the infringement.

121. Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '918 Patent in an amount to be proved at trial.

122. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '918 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

#### **DEMAND FOR JURY TRIAL**

Plaintiff hereby demands a jury for all issues so triable.

#### **PRAYER FOR RELIEF**

WHEREFORE, Taasera Licensing prays for relief against Defendant as follows:

a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of each of the Patents-in-Suit;

b. An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendant, its officers, agents, servants, employees, attorneys, and those persons in active concert or participation with it, from further acts of infringement of the Patents-in-Suit;

c. An order awarding damages sufficient to compensate Taasera Licensing for Defendant's infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with interest and costs;

d. Entry of judgment declaring that this case is exceptional and awarding Taasera Licensing its costs and reasonable attorney fees under 35 U.S.C. § 285; and,

e. Such other and further relief as the Court deems just and proper.

Dated: February 25, 2021

Respectfully submitted,

/s/ Alfred R. Fabricant

Alfred R. Fabricant

NY Bar No. 2219392

Email: ffabricant@fabricantllp.com

Peter Lambrianakos

NY Bar No. 2894392

Email: plambrianakos@fabricantllp.com

Vincent J. Rubino, III

NY Bar No. 4557435

Email: vrubino@fabricantllp.com

Joseph M. Mercadante

NY Bar No. 4784930

Email: jmercadante@fabricantllp.com

**FABRICANT LLP**

411 Theodore Fremd Avenue,

Suite 206 South

Rye, New York 10580

Telephone: (212) 257-5797

Facsimile: (212) 257-5796

Justin Kurt Truelove

Texas Bar No. 24013653

Email: kurt@truelovelawfirm.com

**TRUELOVE LAW FIRM, PLLC**

100 West Houston Street

Marshall, Texas 75670

Telephone: (903) 938-8321

Facsimile: (903) 215-851

**ATTORNEYS FOR PLAINTIFF**

**TAASERA LICENSING LLC**